

victory briefs topic analysis www.victorybriefs.com

Public Forum | November 2013

Resolved: The benefits of domestic surveillance by the NSA outweigh the harms.

Victory Briefs Topic Analysis Book: Public Forum November 2013 – 13PF2-NSA Domestic Surveillance
© 2013 Victory Briefs, LLC

Victory Briefs Topic Analysis Books are published by:
Victory Briefs, LLC
925 North Norman Place
Los Angeles, California 90049

Publisher: Victor Jih | **Managing Editor:** Adam Torson | **Editor:** Adam Torson | **Topic Analysis Writers:** Michelle Keohane, Dave McGinnis, Fred Robertson, Adam Torson | **Evidence:** Rebecca Kuang

For customer support, please email help@victorybriefs.com or call 310.472.6364.

TABLE OF CONTENTS

TABLE OF CONTENTS	2
TOPIC ANALYSIS BY MICHELLE KEOHANE	5
TOPIC ANALYSIS BY DAVE MCGINNIS	13
TOPIC ANALYSIS BY FRED ROBERTSON	24
TOPIC ANALYSIS BY ADAM TORSON	31
AFFIRMATIVE EVIDENCE	39
<i>TERRORISM</i>	39
NSA SURVEILLANCE PREVENTS TERRORISM	39
NSA SURVEILLANCE HAS PREVENTED 50 ACTS OF TERRORISM	40
DIGITABLE SURVEILLANCE IS NECESSARY FOR EFFECTIVE COUNTERROR EFFORTS	41
THE DATA IS VERY HELPFUL TO INVESTIGATIONS	42
SURVEILLANCE IS CRITICAL TO PREVENTING TERRORIST ATTACKS	43
SURVEILLANCE EMPIRICALLY PREVENTS ATTACKS ON THE HOMELAND	44
SURVEILLANCE IS THE LAST, BEST DEFENSE AGAINST TERRORISM	45
SURVEILLANCE IS NEEDED TO PREVENT TERRORISM	46
SURVEILLANCE PROVIDES INFORMATION TO PREVENT A FUTURE 9/11	47
TERRORISM IS A REAL THREAT - SURVEILLANCE IS REQUIRED TO DEFEAT IT	48
SURVEILLANCE WOULD HAVE PREVENTED 9/11	49
ERR ON THE SIDE OF EXPANSIVE INTELLIGENCE PROGRAMS	50
TERRORISTS WANT TO ATTACK THE US BUT SURVEILLANCE EFFORTS STOP THEM	51
ABSENT NSA SURVEILLANCE, THERE WOULD HAVE BEEN MORE ATTEMPTED ATTACKS	52
SURVEILLANCE SYSTEMS EXIST BECAUSE THEY WORK	53
<i>CIVIL LIBERTIES, PRIVACY, AND CONSTITUTIONAL RIGHTS</i>	54
NSA SURVEILLANCE IS LEGAL	54
SURVEILLANCE IS LEGAL AND DOESN'T VIOLATE PRIVACY	55
LOSS OF PRIVACY IS INEVITABLE BUT SURVEILLANCE ENSURES BENEFITS FROM THIS LOSS	56
NSA SURVEILLANCE ISN'T ANY WORSE FOR PRIVACY THAN HAVING A FACEBOOK ACCOUNT	57
PRIVACY CONCERNS ARE NOT JUSTIFIED	58
THE PROGRAM PREVENTS TERROR ATTACKS THAT PRESENT A BIGGER RISK TO FREEDOM	59
CIVIL LIBERTIES ARE WELL PROTECTED	60
<i>GOVERNMENT SECRECY</i>	61
SECRET GOVERNMENT PROGRAMS ARE NECESSARY AND EFFECTIVE	61
EXPERTS WITH ACCESS TO SECRET INFORMATION PROVE IT WORKS	62
<i>A2 ABUSE OF POWER</i>	63
THE NSA IS AN ACCOUNTABLE PROGRAM	63

THERE ARE INTERNAL CHECKS ON PRIVACY LOSS	64
SURVEILLANCE IS LAWFUL AND EFFECTIVE.....	65
THERE IS NO EVIDENCE OF PROGRAM ABUSE	66
ABUSE CONCERNS ARE ENTIRELY BASELESS.....	67
<i>DEMOCRACY</i>	68
SURVEILLANCE DOESN'T UNDERMINE DEMOCRACY - IT HELPS ACTUALLY HELPS IT	68
<u>NEGATIVE EVIDENCE</u>	69
<i>PRIVACY</i>	69
NSA SURVEILLANCE UNDERMINES OUR BASIC RIGHT TO PRIVACY	69
THE PROGRAM IS A MASSIVE INVASION OF PRIVACY	70
MISTAKES THAT CAUSE ABUSE AND INVASIONS OF PRIVACY ARE INEVITABLE	71
<i>ABUSE OF POWER</i>	72
PROGRAM ABUSE HAS HAPPENED BEFORE AND WILL CONTINUE	72
PROGRAM ABUSE IS INEVITABLE	73
SURVEILLANCE INEVITABLY BLEEDS INTO DISCRIMINATION AND PROFILING	74
<i>DEMOCRATIC FREEDOMS</i>	75
SURVEILLANCE HAS A CHILLING EFFECT ON ALL DEMOCRATIC FREEDOMS.....	75
SURVEILLANCE CREATES A CULTURE OF FEAR AND DISTRUST.....	76
SURVEILLANCE DESTROYS ACCOUNTABLE DEMOCRACY AND PRIVACY	77
NSA SURVEILLANCE IS THE DEATH KNEEL FOR DEMOCRACY.....	78
OPEN, FREE TECHNOLOGY IS NECESSARY TO BE AN ENGAGED CITIZEN	79
SURVEILLANCE STIFLES INDIVIDUAL INNOVATION AND FREE THOUGHT	80
SURVEILLANCE CONSTRAINS FREEDOM OF INNOVATION AND EXPERIMENTATION.....	81
SURVEILLANCE UNDERMINES RIGHTS TO FREE SPEECH AND PRIVACY	82
SURVEILLANCE INEVITABLY DETERS TRULY FREE SPEECH.....	83
<i>LEGALITY</i>	84
NSA SURVEILLANCE IS ILLEGAL	84
NSA SURVEILLANCE VIOLATES THE FOURTH AMENDMENT	85
NSA SURVEILLANCE IS AN UNACCEPTABLE INFRINGEMENT OF THE 4TH AMENDMENT	86
SURVEILLANCE VIOLATES CONSTITUTIONAL GUARANTEES OF INTELLECTUAL FREEDOM	87
<i>A2 TERRORISM</i>	88
THERE'S NO EVIDENCE THE PROGRAM IS EFFECTIVE	88
THE PROGRAM IS INEFFECTIVE AND UNDERMINES DEMOCRACY	89
THE PROGRAM ISN'T NECESSARY TO STOP TERRORISM	90
THE PROGRAM HAS NOT PREVENTED ANY ATTACKS.....	91
ATTACKS THAT HAVE BEEN PREVENTED WEREN'T BECAUSE OF THE NSA	92
TERRORIST ATTACKS CAN BE PREVENTED OTHER WAYS.....	93
EMPIRICAL EXAMPLES PROVE THE PROGRAM IS NOT BENEFICIAL	94
TERRORISTS ARE ADAPTING TO AVOID SURVEILLANCE	95
THE PROGRAM IS A HUGE WASTE OF TAX DOLLARS	96
<i>SOFT POWER</i>	97

NSA SURVEILLANCE DEVASTATES OUR INTERNATIONAL CREDIBILITY	97
SURVEILLANCE JUSTIFIES AUTHORITARIAN CRACKDOWNS AROUND THE WORLD.....	98

Topic Analysis by Michelle Keohane

INTRODUCTION

In June of this year, NSA contractor Edward Snowden sparked massive controversy when he revealed the existence of classified government surveillance programs that targeted United States citizens. The story was originally broken to the Guardian, a UK news publication. Snowden reported that through partnerships with private telecommunications companies like Verizon Wireless, the government has extensive access to US citizens' phone and internet data. While we acknowledge that covert surveillance is a crucial part of foreign intelligence operations, it is disconcerting to see it turned towards US nationals. Since Snowden's story went public, there has been a renewed discussion about the conflict between national security and citizens' privacy in this country.

The fundamental tension between security and privacy has been the subject of debate since the drafting of the Bill of Rights. Both the Constitution and the Supreme Court have upheld a right to privacy, but both recognize that that right can be curtailed in certain situations. The conversation about security and privacy has gone in new and interesting directions due to the increase in internet use over the past few decades. Much of our most personal information is transmitted over the internet in private transactions with our internet service providers and other third parties. Corporations like Facebook and Google can track most of what we do on the internet, and even target advertisements directly to us based on extensive knowledge of our search histories and internet browsing. In a world where we accept widespread use of our data for commercial purposes, can our internet lives even be considered private? As technology rapidly evolves, it is difficult for the courts to keep up with the intricacies of digital information storage and retrieval. Where do we draw the line about what is considered private information, as far as the government is concerned? When is it acceptable for the government to use this information? Can it be justified in the face of a public threat like cyberterrorism?

In order to begin to answer these questions, we must first explore the interpretational issues of the topic at hand: Resolved, the benefits of domestic surveillance by the NSA outweigh the harms. This section will discuss the nature of the specific surveillance programs used by the NSA. Next we will turn to a few common arguments for both the Pro and the Con, before considering a few final considerations for successful debates.

INTERPRETATION: What is domestic surveillance by the NSA?

In order to articulate the conflict in the resolution, we must first understand exactly what the National Security Agency does. The NSA was founded on November 4, 1952 under President Harry Truman. It was designed to sustain the United States' excellence in code-breaking after the end of World War II.¹ Since its founding, the agency has served as a central bureau for cryptology as it relates to foreign intelligence and national security. They are responsible for coding and decoding sensitive information to serve the federal government's intelligence purposes.

Today, the NSA still plays a vital role in collecting data that is vital to our national security interests. The agency's function is to "[produce] foreign intelligence through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire, or other electromagnetic means."² In other words, the NSA has the power to track digital communications between foreign agents that are believed to be a threat to national security. The foundation of this power is the Foreign Intelligence Surveillance Act of 1973, commonly referred to as FISA. The FISA Court regulates the use of this information, and ensures that the NSA is in compliance with the statute.

While the NSA focuses mostly on collecting data related to foreign persons, US citizens are not entirely shielded. As per the phrase "domestic surveillance," this topic is limited solely to those instances where NSA surveillance involves communication data from persons on US soil. While the wording of the topic tells us that we are focusing on the NSA, it does not specify the exact nature of its investigations, except that they relate to people within the country. This article will explain three different surveillance programs used by the NSA. All three relate to digital tracking of citizens' data, whether by phone or by internet. It may be possible to investigate other types of surveillance and form case positions around them. However, given the timeliness of the Snowden controversy, I think that the majority of debates will center on digital privacy. Three key surveillance programs that affect US nationals have attracted much attention recently: Boundless Informant (BI), PRISM, and XKeyscore.

Boundless Informant (BI) is a program that allows government officials to track data about citizens' phone conversations, without directly listening to the calls. BI allows the government to collect "metadata," or information about the phone calls, but not their content. However, the information collected is arguably still intrusive; it includes the numbers being called and the

¹ "NSA 60th Anniversary." *The National Security Agency*. 14 December 2012.
http://www.nsa.gov/about/cryptologic_heritage/60th/index.shtml

² "The National Security Agency: Missions, Authorities, Oversight, and Partnerships." *The National Security Agency*. 9 August 2013, p. 2.
http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf

duration of the conversations, which allows the government to track calling patterns. If the metadata arouses suspicion for any reason (for example, calls to a phone number that belongs to a suspected terrorist on foreign soil), intelligence officials can then go to court to retrieve a warrant to monitor the content of the conversations.³

PRISM is another surveillance program that is intended for use only against foreign suspects. It can track the content of internet transactions, whether those are messages sent and received, videos uploaded, or other content shared.⁴ The program uses partnerships with Google, Yahoo, and Microsoft to collect data. Since the Snowden controversy, all three companies have issued statements announcing that they only give up data when legally required.⁵ Though the program is meant to track individuals outside of the United States, collected data can implicate people inside of the country. For example, a citizen's data could be analyzed by the NSA if he or she was copied on an e-mail between foreign suspects.

Perhaps the most far-reaching program is XKeyscore, which has the ability to track the content of virtually all online activities of US citizens. The Guardian published an NSA PowerPoint presentation from 2008 briefing officials on the use of the program. The presentation lauded the expansive powers of the program. In response to the article, the NSA asserted that while the XKeyscore has the power to find very personal information, in practice it is carefully monitored and accessed only by officials whose direct tasks require its use. The program is allegedly subject to a series of checks and balances within the agency.⁶

In the context of the debate round, it will be more important to understand the general functions of these programs, rather than their specific nuances. Even if you do not use them by name in-round, it is essential to understand metadata and the extent of government access to online communication. The nature of the programs will provide a foundation for the types of arguments you make on both sides. It can also help you frame the round favorably on both Pro and Con.

³ Richard Lempert [Visiting Fellow in Governance Studies at the Brookings Foundation and the University of Michigan's Eric Stein Distinguished University Professor of Law and Sociology emeritus], "PRISM and Boundless Informant: Is NSA Surveillance a Threat?" *The Brookings Institute*, 13 June 2013. <http://www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert>

⁴ Lempert, "PRISM and Boundless Informant."

⁵ Barton Gellman and Laura Poitras [Pulitzer Prize-winning journalist, documentary filmmaker], "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program." *The Washington Post*, 6 June 2013. http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers/3

⁶ Glenn Greenwald [journalist and political commentator], "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," *The Guardian*. 31 July 2013. <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>

It may also be worth noting that the NSA has been in the public eye more than once in the last few years. In 2007, the agency was under scrutiny for collecting illegal phone data under the USA Patriot Act. It came to light that between 2001 and 2007, the Bush administration authorized warrantless wiretapping of suspected terrorists on and off of US soil. Warrantless phone-taps were widely (and legally) condemned as a result of the controversy. I imagine that most debates will center on more recent events and policies, but it is worth knowing the background information of these types of government actions. I mention the older conflict here to underscore the importance of finding timely sources on this particular topic. An article about a similar topic written in 2006 will cover vastly different issues than one from this year.⁷ Once we have a firm understanding of the contemporary landscape of domestic surveillance, we can turn to the arguments in favor of its use.

PRO: What are the benefits of domestic surveillance?

The most obvious and compelling Pro position is that NSA surveillance of US citizens thwarts terrorist attacks within our borders. The NSA has released data to this effect, commonly stating that 50 attacks have been foiled as a result of information secured from legal data tracking. Evidence citing foiled attacks will be essential in any Pro case. In addition, Pros may wish to discuss the threat of cyberterrorism, terrorist attacks that originate online. It may be compelling to argue that online surveillance is the best way to prevent these types of attacks. In either case, the Pro must keep in mind that the topic is specific to domestic surveillance, so investigating the online or cell phone activities of *people within the United States* must be a critical part of stopping terrorism in the Pro world. If the team can establish this, they have won a very compelling impact story. The key to success on the Pro will be emphasizing tangible positive effects of security policies that keep Americans safe.

Though case positions about the prevention of terrorism will undoubtedly be common, they are not without their flaws. First of all, any data about the effectiveness of the NSA will be, by and large, from the NSA itself. This is due to the secretive nature of their operations; the agency is not subject to outside assessments due to the sensitive nature of the information at stake. The second problem is that prevention of a terrorist attack is a question of a “dog that didn’t bark.” In

⁷ For more information on the 2001-2007 wiretapping incidents, see: “Domestic Wiretapping in the War on Terror: A Briefing Before The United States Commission on Civil Rights.” *United States Commission on Civil Rights*, January 2010. <http://www.law.umaryland.edu/marshall/usccr/documents/cr12d2010.pdf>. In addition, the Wikipedia page for “NSA warrantless surveillance (2001-07)” has extensive footnotes with various resources about the controversy. (Read and cite the sources, not Wikipedia!)

other words, it is difficult to prove that an event *would have* taken place without the use of domestic surveillance. If the NSA is doing its job correctly, nothing happens. Con teams may be quick to point out that there could be any number of alternate reasons that terrorist attacks have not occurred. It is difficult to attribute direct causation to NSA surveillance, especially since the topic is specific to surveillance of people within the US. I do not see any single, knock-out response to these criticisms. However, the best-prepared Pro teams will have thought over these critiques and figured out how to leverage against them.

Another important Pro consideration will be to establish terrorism as a present and on-going threat. If the Con team can successfully prove that the likelihood of a terrorist attack is low, it will be difficult for the Pro to argue that surveillance is essential to prevent an attack. In order to prove that surveillance of persons on US soil is more beneficial than costly, it must be a solution to a clear and present danger.

It is also in the Pro team's interest to downplay the invasiveness of NSA tactics. While these types of arguments are fundamentally defensive in that they do not lay out tangible benefits to domestic surveillance, they can be very effective in undercutting the Con team's harms. The Pro team will likely want to frame surveillance as a minor occurrence that law-abiding citizens need not fear or even think about. As the common saying goes, "those with nothing to hide have nothing to fear."

CON: What are the harms of domestic surveillance?

The Con offers a bit more variety than the Pro. The first line of defense for the Con should be disputing the efficacy of NSA surveillance in stopping terrorist attacks. This should be a part of every debate for successful Con teams. Since prevention of terrorism is the most compelling offense for the Pro, to allow it to go unchallenged would be leave the door open to a persuasive Pro story about the importance of saving lives.

There are a few different ways to criticize the efficacy of the NSA. Some have disputed the legitimacy of the commonly cited studies that claim surveillance is effective.⁸ Another common criticism is that collecting so much data can lead to an information overload that will inhibit the effectiveness of intelligence operations. A third approach may be to explain how NSA tactics trade off with other, more effective counterterrorism measures.

⁸ A commonly cited success story for NSA surveillance was the prevention of a New York City subway bombing by Najibullah Zazi in 2009. Popular news sources have questioned whether NSA involvement was necessary to thwart this plot. It is probably worth your time to investigate both sides of this case.

When we consider the fundamental clash of the resolution as a question of security versus privacy, the next clear Con position relates to the importance of privacy rights.⁹ The Fourth Amendment is consistently cited as a codification of the right to privacy in the United States. It reads, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Our “papers and effects” take a different form now than they did when the Bill of Rights was drafted. This topic gives us an interesting opportunity to consider how the spirit of this amendment can be transferred into the Information Age.

The violation of privacy rights seems intuitively and implicitly important, but when compared with a Pro story about lives lost to terrorist attacks, it may become difficult for the judge to prioritize. As such, it will be important for any privacy rights position on the Con to clearly explain the implications of an abuse of these rights. I would advise that Cons avoid a “slippery slope” argument about how violating privacy can “open the door” to further rights violations. Positions like these are commonly overstated; minor civil rights infractions have happened in this country with some frequency, and we have not yet become a totalitarian state. Any arguments about government abuse of power must be more nuanced than that. The best form of this argument will be specific to citizens’ digital privacy and the government use of this data. It will also make an argument about why the government has some sort of incentive to grab up more power or abuse rights. Another possible form of the argument may be to claim that the availability of this data is inherently problematic. Perhaps the government does have our best interest at heart and earnestly seeks to protect our privacy. What if the system was somehow compromised and that information became available to other parties? Does this matter when private third parties already have much of our information? These are questions worth exploring.

Another way to articulate the implications of privacy violations is through an argument about speech chilling. The premise is that US citizens will alter their online behavior as a result of the knowledge that their digital conversations may be monitored. The implication is that free expression, another constitutional value, will be hindered as a result of surveillance. This may lead to a hesitation to challenge the government or engage in unpopular disputes, which is also harmful to US democracy. This argument is also difficult to prove beyond a doubt, and Con

⁹ The following article provides an in-depth discussion of privacy rights. However, it should be noted that the article is from 2002 and is not the best resource on the most recent conflicts about data privacy. Daniel J. Solove [Assistant professor of law], “Digital Dossiers and the Dissipation of Fourth Amendment Privacy.” *Southern California Law Review*, Vol. 75, 2002, pp. 1083- 1168.

teams wishing to employ this strategy also need to be able to provide concrete harms of a loss of free expression, once again to be weighed against the potential loss of life in the Pro world.

A final potential harm of domestic surveillance relates to unjust profiling. Since September 11, police and government targeting of Muslim and Arab Americans, among other groups, has become a widespread problem. A Con team could argue that allowing surveillance of people living in the United States will only increase unfair profiling of innocent individuals who have connections to the Middle East.¹⁰ If we view the topic through the lens of digital privacy, racial profiling by sight will not necessarily be a relevant issue. However, it is still possible to profile based on associations with people outside of the United States, and this can still lead to unjustified violations of privacy.

TO CONSIDER ON BOTH SIDES:

I would like to present two further issues that may be relevant to strategies on either side. The first is whether or not US citizens approve of domestic surveillance programs. I think there will be evidence available to support either side of this claim. However, I am not sure that it directly relates to the questions of comparing harms and benefits. It would seem to me to be an overcomplicated link chain to try to draw a tangible impact from how the population feels about the actions of the NSA. While this is certainly a relevant concern as the issue is debated in the real world, given the wording of the resolution I don't see this type of argument doing much for either the Pro or Con.

Second, even though the topic specifies domestic surveillance, I would encourage debaters to consider the international implications of these US policies. I believe there may be arguments to be made about how our foreign intelligence allies would react to our use of surveillance techniques against our own citizens. Would they accept such treatment of their own citizens? Will they still be willing to collaborate with us knowing that we use these practices? Will a terrorist attack only take place in or affect the United States? The scope of the topic can be expanded in interesting ways if we consider the implications of United States actions on the rest of the world.

CONCLUSION

The most successful debaters on this topic, whether Pro or Con, will find a compelling way to weigh between the concrete harms of loss of life due to domestic terrorism, and the more wide-

¹⁰ The Briefing from the US Commission on Civil Rights, cited in note 7, also provides some information about this issue.

reaching but perhaps nebulous implications of harming civil liberties. Perhaps the Pro has a more tangible impact story, but the Con has the ability to challenge the efficacy of NSA surveillance and find creative ways to compare and weigh their harms. In order to make the judge's decision process easier, it will be essential for debaters to invest time in comparing the Pro and Con worlds.

One of the most exciting prospects of debating this topic is that it will continue to develop as the month goes on. Articles about NSA policies are being released on news sites every day. The most successful debaters will respond to the changes in our national dialogue about this subject. Never forget the centuries-old clash of security and privacy, but remember to stay up to date on the intricacies of this new dispute.

Topic Analysis by Dave McGinnis

The first thing that should jump out at you about this topic is that it is even more “ripped from the headlines” than PF topics are generally. So doing solid *research* on the nature of the NSA’s domestic surveillance is going to be a huge part of your preparation. You need to know a lot of important facts, including at a minimum:

- 1) How the NSA surveillance information became public;
- 2) What facts about the NSA surveillance program(s) are known; and
- 3) All of the arguments made for and against the actions taken in those programs.

There is a *lot* of misinformation out there about what the NSA has and hasn’t done. Debating this topic is going to be a tough needle to thread because not only do you have to make sure you know all of the *actual* information, but you’re going to need to have a good sense of what *inaccurate* information is available because (and this is the really tricky part) *your judges are going to believe some of the inaccurate information*. More important, many of your judges are going to have strong opinions about the topic *based on* their inaccurate information. If you challenge their strongly held views too abruptly you may end up losing ballots. For example, one very good argument for the affirmative of the topic is that privacy in general, or at least the kind of privacy “invaded” by NSA surveillance, is not terribly valuable in the modern age. That argument is sound on its merits, but may well anger a lot of judges -- from both sides of the political spectrum.

NATURE OF NSA DATA COLLECTION

A key part of the debates is going to be doing solid research on the nature and scope of NSA data collection and usage. This is going to be a tough job for a couple of reasons. First, there are a number of different NSA programs currently at work that are now or have been recently subject to news reporting. And second, both news reporting and online discussion of these programs is often very confused -- that is, it’s difficult for a lot of people to keep track of which program does what. For example, the most recent scandal involving information leaked by Edward Snowden was prefigured by a smaller-scale revelation in 2006 about an NSA program called *Mainway* that logs and graphs billions of pieces of data per day about communication among Americans and foreigners over telephone, cell phone, and internet. Also, there was a high-profile scandal in the early 2000s about the Bush administration authorizing warrantless wiretaps, also carried out by

the NSA, but which were eventually ruled unconstitutional and (purportedly) ended. The tricky is that whole books could be (and have been) written about both of those scandals, and in-depth research into Mainway and warrantless wiretapping will really only scratch the surface of the factual background on this topic.

So what exactly does the NSA do? It's not entirely clear, partly because some of the information about NSA activities hasn't been released yet, and partly because different sources make different interpretive claims about the information that *has* been released. ***You need to do solid research on this question.***

A very general overview might look something like this:

The National Security Agency is the U.S. intelligence bureau tasked with conducting "signals" intelligence work -- that is, collecting data and managing data streams clandestinely. Basically, their job is to listen in on the electronically-carried communication of foreign targets for the purpose of decoding and tracking and keeping an eye on the bad guys. They get to do this in secret, and they can track foreign citizens' communications even if they are residing in the United States.

The fact that the NSA collects lots and lots of communication data is not by itself controversial (at least in the U.S.) That is their job. The bulk of the controversy has erupted over the NSA's ability to track data of *Americans*, because we have a natural (and constitutionally-supported) expectation that the government is not spying on *us*. The Constitution protects us against "unwarranted searches and seizures," so if the government wants to surveil an American citizen, the expectation is that they will go through a rigorous process of obtaining a warrant. That idea is complicated further by the existence of the Foreign Intelligence Surveillance Act (FISA), a law that allows the NSA and other government agencies to surveil foreign entities and their agents (even if those agents are U.S. citizens) who reside in the United States. FISA was necessary to allow *any* covert monitoring to go on inside the borders of the U.S. -- it is understood that the government can and does carry out covert surveillance outside the U.S.

Post-9/11, the FISA law was heavily restructured to make surveillance easier. A separate FISA court with warrant-issuing power has existed since 1978, but the volume and regularity of FISA warrant issuance increased drastically after 9/11.

The general shape of the controversy over NSA monitoring is about their collection and analysis, through a variety of programs, of communications "metadata" relating to American citizens. Metadata are pieces of information about our electronic communications -- who called, emailed,

texted, tweeted at, posted on the same discussion board as, etc., whom. Given the volume of electronic communication that takes place every day in the U.S., there is a massive stream of billions or even trillions of pieces of metadata generated every day. While the NSA doesn't generally "listen in" on individual communications (and there is some question about whether they have the ability to do this), they are capable of graphing communication interactions and intersections to generate a tremendous amount of information about individual people. Since the tracking of information about potential terror suspects inevitably leads to communications between foreign nationals and American citizens, the NSA collects massive amounts of data on American citizens. The NSA can, for example, tell a lot about who your friends and associates are, what your activities are, what your business is, etc., just by generating graphs that detail the web of your electronic communications. Even creepier, perhaps, is that call metadata for cell phone users includes *locations*, because cell phone signals "ping" off of individual cell towers, so along with all of the other information that the NSA can gather about you, they can track your movements using only call metadata. Further, while the law places limits on what the NSA can supposedly do with this mass of information, the Snowden leaks reveal that the NSA has fairly regularly gone beyond its legal limits in "peeking" at data on normal U.S. citizens.

The reason the NSA wants to collect all this data isn't just because it's a creepy government organization. The NSA is involved in a process called *data mining*, which basically means looking into massive streams of data for individual threads of information that can lead to useful investigations of foreign threats. It's easy to villainize the NSA because they are secretive and creepy and because they appear to be breaking the law at least some of the time. But bear in mind that the NSA is tasked with signals intelligence in the service of American national security - that is, the only reason they officially want all this data is so that they can identify foreign threats (be they governmental or non-governmental, like terror organizations) and deal with them, preventing harm to U.S. citizens.

Your research should prepare you to discuss intelligently, at a minimum, the following concepts:

- The National Security Agency and "signals intelligence" generally.
- The Foreign Intelligence Surveillance Act
- Edward Snowden (including, but not limited to, reading the original articles in *The Guardian* and other publications)
- PRISM
- ECHELON
- Warrantless wiretapping (Bush-era program)
- MAINWAY

AFF ARGUMENTS

Digital privacy is (A) not important and/or (B) doesn't exist.

The negative has a strong argument in the defense of privacy, which is an important right. Some affirmatives will argue that there is no constitutional right to privacy because the Constitution doesn't actually mention "privacy." This is not a good argument because there is a long history of interpretations of the Constitution such that privacy is an important "penumbral" right, most importantly deriving from the Fourth Amendment. A better argument against the concept of privacy on this topic is to attack the idea of *digital* privacy. That is, the NSA programs have only peered into the digital / electronic / phone communications of American citizens, and those kinds of communications are not "private" in the sense that a conversation in the home is private. This is true because the most common legal definitions of privacy refer to *reasonable expectations* of privacy -- that is, a communication is private if it is made at a time and in a place where a reasonable person could expect to be unobserved. So, for example, if you share a confidence with your spouse in your bedroom at home and someone is listening in with an electronic bugging device, you could say that they had violated your privacy because you reasonably expect communications in your home bedroom to be unobserved by others. However, if you share the confidence with your spouse in a public square and are overheard by a passerby, you can't complain that your privacy has been violated because you could not reasonably expect that you would be unobserved.

The argument for the aff here is that the digital realm is not someplace where we can reasonably expect to be unobserved. When we send an email or text through the air we do so knowing that the technology to observe it is fairly commonplace, and even if there is no technology involved, we can't know that when the recipient opens the email or reads the text there won't be someone standing near them to observe it. Electronic communications are sent out into the world on air waves or through cables over which we have no direct control, and therefore, no reasonable expectation of privacy. That means that the NSA's programs for monitoring and cacheing electronic data are not violations of privacy.

This, of course, is a defensive argument. Proving that the NSA programs don't violate privacy is not a reason you should win the round. However, privacy violations will be a common negative argument so having solid arguments against the privacy debate is probably a good strategy.

Domestic surveillance by the NSA has stopped lots and lots of terrorist attacks.

This is obviously the best and most important argument for the affirmative. Several commentators -- military and congressional -- came out in the wake of the Snowden revelations and defended the NSA on the grounds that the intelligence gathered through the various programs has been key to preventing terror attacks.

One problem you'll run into in researching this argument is that much of the information about specifically what terror attacks were prevented and how they were prevented is probably still classified, so the comments from people who have reason to know are necessarily vague. That said, you'll probably be able to find enough evidence in mainstream media sources that combines the actual comments of policymakers and military leaders with analysis and extrapolation by journalists and wonks to establish that there has been a real benefit to counter-terrorism efforts from the NSA programs.

You might also spend some time discussing in the abstract how NSA data-mining makes sense as a powerful tool to track terrorists. Terror networks achieve their goals through stealth, or through "asymmetrical" attacks -- that is attacks against a more powerful military adversary that take advantage of structural weaknesses (like lapses in security) when the adversary doesn't have the military force necessary to take the U.S. on directly. Communication is a key element of terrorists' strategies. Email, websites, bank transfers, cell phone calls, etc., are all a huge part of how terror cells organize and plan to carry out attacks. Covert monitoring of massive amounts of call and internet data allows our intelligence agencies to connect the dots between terrorists we know about and hidden terrorist resources, and this allows them to trace down planned attacks and prevent them.

The real nature of the NSA surveillance is not as bombastic as the media have portrayed it.

The trick about this argument is that it isn't actually an argument per se -- that is, it's not offense. But it's really important that you clarify the nature of the actual NSA program(s). Based on media portrayals, a lot of Americans firmly believe that NSA spooks are listening to all of your phone calls and reading all of your emails. That is not true. The process the NSA is involved in is called "data mining," and it involves coordinating vast amounts of meta data to look for connections that would point NSA spooks in the direction of potential terror suspects -- connections that justify warrants for actual searches.

The violations of privacy involved in this data mining are highly technical, and not terribly personal. This doesn't necessarily mean they aren't problematic at all, it just means that the violations aren't the kind of visceral attacks on personal privacy that the average person has

been led to imagine. The NSA isn't supposed to be looking at even metadata of American citizens without warrants from the FISA court, and it's clear that (A) they have been looking at a *lot* of metadata *with* warrants and (B) they have *occasionally* been peeking at data without warrants (though it also seems to be the case that most of those violations have been accidental, and have been quickly reported.)

The NSA agents who observe your data do not know or care who you are. In fact, they observe data representing so many hundreds of thousands of individuals that it would be impossible for them to have the time to poke into the specific private details of some person's life if there were no evidence pointing to a tie to terrorism. This isn't to say that the NSA doesn't have the technical *ability* to read individual emails or listen to individual phone calls. The PRISM program collects and stores vast swaths of internet traffic, including (but not limited to) details on what websites have been visited, who has emailed whom, and the content of their email / Facebook / whatever messages. The point is that the NSA collects *so much* of this data that it's not within their purview or in their interest to be poking through any particular individual's materials unless there is some reason (connected to a terror investigation, for instance). The sheer amount of data that is collected, far from being a "smoking gun" about the NSA's abuse of your privacy, is actually a reason why the "privacy violations" are nominal at best. The NSA collects a massive hay stack, and we are each only tiny needles.

You might also point out -- with evidence -- that the NSA is only permitted, currently, to look at email or other communications where one end of the communication exists outside of the U.S. The purpose of NSA data collection is still monitoring foreign intelligence sources. The requirement that their electronic takings originate or terminate outside the U.S. ensures that they remain constrained by that rule. (Be careful how heavily you lean on this argument, though, because leaked documents have shown that the NSA bolloxes this particular restriction up fairly regularly.)

NEG ARGUMENTS

Loss of privacy

The most basic negative argument has to be *loss of privacy*. Many debaters are going to talk about the loss of privacy without spending *any* time developing arguments about why that matters. They will count on judges having knee-jerk reactions in favor of privacy. But it's not immediately clear why a loss of privacy is a concern -- especially if the aff is making a compelling case that the trade-off for the loss of privacy is the prevention of large-scale terror attacks that

could kill thousands upon thousands of Americans. That means that a *good* privacy neg position is going to include a well-developed discussion of just why privacy is important.

There are a lot of philosophical and psychological arguments about the importance of privacy. The best ones will talk about how privacy is key to the development of the human personality. People need to have a sphere of privacy -- a bubble in their lives when they know they are unobserved -- so that they can be open and honest with themselves about their own personal characteristics and appetites. When we know others are observing us, we tend to be on guard about our expression. We will edit what we say or write, who we associate with, where we go, etc., based on how we *want others to perceive us*. Under constant observation it would be impossible to develop or express an authentic personality because we would forever be afraid of others' judgments of us, and would censor our expression and activities accordingly. Privacy allows for the development and flourishing of the human personality because it allows us to be honest to *ourselves* about our preferences, thoughts, and beliefs. Without privacy, it would be difficult or impossible to be an authentic human being.

Clandestine government surveillance threatens this privacy. Particularly when the surveillance programs are cloaked in secrecy, they create a sense in the public that they are always being watched one way or another. If you know that the government has the ability to monitor what you read, for example, you might be careful about what books you buy or check out of the library. One old saw from spy movies of the 1990s is the idea that the government tracks book purchases and library borrowing, and will, for example, begin investigating you if you check out both a copy of the Qur'an and a book on explosives. (Both *Se7en* and *Enemy of the State*, classic 1990s thrillers, include some version of this as plot points. Irrelevant to the topic, perhaps, but you should see those films.) If that were true, then people who happen to be interested in those two subjects would have to censor their reading preferences to avoid getting in trouble with the government. Extrapolate that *kind* of thing to a million different decisions about communication and media consumption, and you can see how a robust government surveillance program could easily become very oppressive.

International fall-out

In one sense the topic is too limiting, because it specifies *domestic* surveillance. The recent NSA leaks also included information about NSA spying on foreign leaders, and that has led to significant international political fall-out. For example, at the meeting of the United Nations general assembly in September of this year, Brazilian President Dilma Roussef used her entire speech time to rail against the United States and its spying efforts after it was apparently revealed that among the targets for secret email reading were her personal email accounts.

European Union nations have also expressed concerns and there was some concern that the controversy would scuttle important trade negotiations between the US and the EU. The implications for soured international relations are broad and there is certainly a great deal of evidence on this question.

Of course the affirmative will (and should) counter that the resolution is specific to *domestic* spying programs, and obviously these international implications fall outside that. The negative might argue in return that the program is part and parcel of the same problem, and that the revelations about the domestic program were tied to the revelations about international spying. This is a reasonable interpretation because the NSA's whole justification for spying on US citizens under *any* circumstances is that they looked at those communications only when they were connected to communications with foreign citizens. So, in that sense, it's impossible to tease the domestic and international implications of the NSA program apart. If the negative presents this argument carefully, I think most judges should be persuaded.

Snowden himself

Snowden himself has created a number of important problems for the United States. His actions and the support he has received from factions of both the political right and left in the US have been embarrassments to the Obama administration, and have also complicated politics because traditional allies on both sides of the aisle are split on the validity of the NSA programs. After all, many of these programs date back to the Bush era and even earlier -- it is difficult to hang them solely around Obama's neck. Further, the NSA programs are designed to basically subvert individual privacy rights to a primary national security concern -- and Republicans are traditionally national security hawks, so complaining that the Obama administration is "too committed to national security" is not something that the Republican mainstream wants to do.

There is a more straightforward concern about Snowden, however. His status as a human rights refugee in Russia is a huge problem for the United States, for two reasons. The first is that it complicates our relationship with Russia. Whether you like the NSA program or not, it's pretty clear that Russia is much tougher on human rights than we are. Vladimir Putin is essentially a new-era Soviet-style dictator, who has manipulated the Russian political system to guarantee his own ascendance in perpetuity. Yet he is cast now as the protector of Edward Snowden's basic human rights, as though if Snowden were to return to the U.S. he'd be tossed in some kind of gulag. Snowden's decision to flee to Russia and now Russia's decision to treat him as a human rights refugee makes it much harder for the United States to maintain a collegial relationship with Russia. The fact that Russia is sheltering Snowden is an implicit statement on Russia's part that

the United States is an active abuser of human rights. It is difficult to maintain a sunny relationship between the nations with that as backdrop.

The implications of a souring relationship between the U.S. and Russia are many, and have to do with important areas of geopolitics. You can explore a number of different possible implications, but I'd hazard a guess that the most important will have to do with trade and political stability in the Middle East. Syria is a good example that you might cite of a situation where the inability of Russia and the U.S. to see eye to eye is contributing to massive human casualties in the short term and, potentially, to a more drastic set of harms in the long term.

The second problem stemming from the Snowden situation is that it erodes the United States' credibility as a global leader on human rights issues. Adversaries of the U.S. can easily spin this story to suggest that we are hypocrites when it comes to human rights issues -- that is, we criticize other nations for failing to live up to liberal standards of human rights provision but at the same time we are monitoring our own citizens and hounding the government whistle-blowers who call us out on it. Of course, it's ridiculous to suggest that the U.S.' use of covert electronic monitoring to track potential terrorists is tantamount to the kind of political repression we see in places like China, Russia, or Iran -- places where simply being a member of the opposition party can result in being thrown in prison, or where subscribing to a proscribed religion can result in government harassment or detention. But the Snowden situation is terrible for America's "optics" -- that is, the perception of the political situation as opposed to its foundational reality.

The impact of this isn't just that America looks bad, or that we can't hold our heads up high, or whatever. Rather, the implication that really matters is that the U.S.' leadership on international human rights has the potential to have a positive impact by setting rights-positive norms, creating international expectations that rights overall will be respected. Obviously this isn't a black-and-white, 100% kind of deal -- it's not that "everyone will respect rights because the U.S. says so." Rather, leadership and norm-setting is a gradual practice that leads, in the long term, to gradually improving human rights protections. Eroding the U.S.' leadership position in this area by making it seem as though we are just another state abuser of human rights reduces our capacity to drive rights norms in a positive direction. In the long run, more people will suffer as a result.

Constitutionality

The Constitution's fourth amendment contains an explicit prohibition against "unreasonable search and seizure." The NSA program is clearly unconstitutional by that standard because it permits the government to conduct searches of electronic documents without a warrant -- or, really, without even any individualized suspicion. The government has tried to get around this

problem with the use of FISA courts that grant warrants very liberally and in secret, but the NSA program has gone well beyond that -- there is significant evidence of the NSA searching electronic data without FISA warrants.

If you're going to make this argument you need to frame the debate in such a way that violations of the Constitution matter. "Constitutionality" is, for lack of a better term, a *deontological* argument. That is, it's an argument that there is a set moral rule -- the Constitution -- and that the act is wrong *solely because* it violates the moral rule. Don't be confused by the overlap between deontological warrants and teleological impacts -- that is, it's easy to argue both that *it is wrong to violate the Constitution* and *violating the Constitution* (or "this violation of the Constitution in particular") *will lead to bad outcomes, and thus is wrong*. Those are different arguments entirely.

Next, the affirmative will likely respond to this argument by pointing out that the resolution appears to call for a utilitarian judgment -- that is, the resolution calls on us to compare harms and benefits. This sounds utilitarian-ish, but there's no reason "harms" and "benefits" can't be harms and benefits to the fabric of the Constitution. If you're doing a good job with a Constitutionality framework, you should be able to convince your judge that a violation of the Constitution counts as a harm.

Loss of trust in government / transition to the "big brother" state

If you haven't read the novel *1984*, you should go out and grab the Cliffs' Notes version (or, at least, read the Wikipedia summary.) That novel depicts a dystopian future in which the government (A) has highly restrictive laws on its citizens' communication and interaction with others, and (B) maintains strict surveillance of all citizens at all times via two-way TV screens built into the walls of citizens' apartments. The government uses its power to constrain and direct the lives of the citizens. And, there's torture and stuff.

This idea of the government becoming overwhelmingly intrusive in the name of national security is ingrained in the culture. The NSA surveillance scandal plays directly into this literary/philosophical theme because it suggests that the government has decided that it can almost literally reach into our homes (through our phones and computers) to observe our communications. The parallel to the Orwell novel is almost chilling. And, of course, the government justifies its actions in the name of national security.

The affirmative will argue, correctly, that the government's purpose in collecting all of this data is a noble one. It is not trying to squelch our communication or control our lives; it is just trying to

track down terrorists. But there are a couple of problems with that argument that the negative can easily exploit:

(1) Even if the government isn't misusing this power now, the fact that it *has* the power, and the further fact that it maintains and uses this authority *in secret*, means that the checks and balances of democratic governance have failed. It is supposed to be the case that the government *cannot* abuse our rights, not solely that they *elect not to*. This kind of secretive state authority to violate rights is wrong even if it's not being misused in moment, because by the very secretive nature of it, there is no check in place to prevent it from being misused at some future time.

(2) Even if the government never plans to misuse the information, the fact that they are gathering it has a withering effect on public trust in the government. This is made worse by the fact that the NSA programs are bipartisan -- both Republican and Democratic administrations have engaged wholeheartedly in the collection of these data. It's as though there is no one left whom you can trust.

Topic Analysis by Fred Robertson

Overview:

This resolution presents some difficulties to Public Forum debaters because it is not at all easy to find research which clearly supports “domestic surveillance by the NSA.” First of all, the NSA claims that very little domestic surveillance takes place, unless there is lots of proof that communication from a foreign location has first occurred, and that this communication is proven to be from a source that is “suspect” of possible terrorist activity. The agency admits that meta-data has to be analyzed first (such as phone call records or email logs) in order to lead to the discovery of suspect communication with foreign sources, but says that such searches are not really surveillance since people have no expected privacy protection for things such as phone numbers called or email addresses emailed. Court decisions back up this perspective. The phone companies and internet providers have been quite willing to turn over their records and really have no choice in the matter.

Therefore, some affirmatives might narrow the debate ground by arguing that most of what civil libertarians are calling surveillance isn’t really surveillance. According to Merriam-Webster’s online dictionary, surveillance is “the act of carefully watching someone or something especially in order to prevent or detect a crime.” The pro can argue, fairly logically, that having a computer sweep phone or email records to determine if there are frequent communications with foreign sources which are suspected of links to terrorism is not really “carefully watching” someone. Although the NSA admits that mistakes have been made, as far as incorrect determinations of suspect foreign sources of communication, or putting US only communication under surveillance, it says it has found out those errors and corrected them. Defenders of the agency argue that the agency has been vigilant in identifying any overstepping of strict boundaries, and keeps most US citizens from actually being placed under surveillance. Your phone records and emails may be checked, but that’s all that happens. Actual “careful watching” that constitutes surveillance—called “targeting”—only occurs once many red flags in your patterns of communication are identified. That needs to happen, it can be argued, in order to prevent possible terrorist plotting. The affirmative then gives examples of how that sort of targeting has prevented terrorist acts. There are the benefits, and the costs to American’s privacy are minimized. Seems simple. The problem for the affirmative is the step in which the affirmative “gives examples of how that sort of targeting has prevented terrorist acts.” NSA chief General Keith Alexander recently testified to Congress that the number of actual “terrorist plots” identified and allegedly prevented in the United States was 13. I have been searching for details of these plots, as far as proof of capability-- that the people plotting had any means to carry out their plots or had contacts with others who were helping them gain those means—and find such details very hard to find. It’s easy to say “I want to blow up the New York Stock Exchange” and ask someone else how to do

so, via the phone or internet. It's much more difficult to engage in meaningful planning to get that mission funded and accomplished. There simply isn't much tangible evidence that the programs the NSA claims have yielded great security benefits have led to arrests of terrorists in the US working on realistic plots to do harm to Americans. That's a problem for an affirmative that needs to prove benefits of NSA "domestic" surveillance.

The negative also has problems with establishing tangible harms. If the NSA has a computer sweep my phone calls and emails, they will see that I do contact some people in foreign countries. These people almost certainly aren't suspected of terrorism, so that ends any government intrusion into what I am communicating. It is probable/possible that the emails may be more problematic, as would be text messages, since computers could search the words used by me in these emails and text messages, and I am a former debate coach. Therefore, discussion of weapons of mass destruction, anarchy, or terrorism could pop up fairly frequently. Maybe I would get a closer look, briefly, by some computer program. But that would be about it, most likely. Even though there would be no reasonable suspicion that would justify the brief look, it seems difficult to argue that the brief look would cause me real harm.

An additional problem with this resolution is trying to determine how much NSA domestic surveillance costs. No one in the US government will actually admit how much the NSA costs since it is funded under a "black budget" which is highly classified. There are estimates available, of course, but they are just that: estimates. They come from documents leaked by Edward Snowden. According to an August 19, 2013 Seattle Times article by Associated Press writer Stephen Braun, "The latest revelations also disclosed limited details about the highly classified 2013 intelligence "black budget," which previously only provided a topline of nearly \$53 billion. The \$52.6 billion intelligence budget described by the Post discloses that the NSA's portion was \$10.5 billion in 2013 - outstripped only by the CIA's \$14.7 billion." Since you will be debating, and people who debate, like most Congresspeople, regularly distort facts, you can expect to hear the 52.6 billion figure used frequently as the cost of NSA domestic surveillance even though that clearly isn't the case. The reality is that only a few people know what the NSA's domestic surveillance costs and they aren't telling.

One thing that can happen, when there is so little proof of tangible harms and benefits, as is the case with NSA domestic surveillance, is that people decide to talk about less tangible harms and benefits, which I will deal with in the next section.

Framework:

One tactic might be to set up a framework for debate that says, essentially, "let's do this debate like a very old school Lincoln-Douglas debate." By this, I mean to say that a team could argue that we ought to decide whether domestic surveillance by a government agency harms or helps important values. Don't ask Lincoln-Douglas debaters who debate "national circuit" style to help

you with this; they don't have any idea what debating like this is and would consider such arguments-- about how warrantless searches harm values like freedom of thought, association, and speech-- mundane and "stock." Pretty much every sophomore national circuit LDer believes such concerns beneath his or her intellect. But in ancient days of Lincoln-Douglas debate, debaters would argue about how values underpin constitutions, laws, and policies. They argued that when values come into conflict, as they frequently do, thinking people have to do the hard work of determining which values take priority. In other words, we have to decide when one value can be reduced in priority, or sacrificed, to some extent, because another value is more crucial.

The resolution clearly sets up a value conflict between freedom and security. Those two things both are quite important, so deciding which value needs to give is not easy. Still, this determination is crucial to the debate. Is the sacrifice of freedom justified because of the gain in security? Do security justifications trump pleas to be left alone when a government is functioning in a just manner? Even if we have willingly submitted to warrantless searches at airports by a government agency, the question is whether or not we should be doing this, and the answer largely depends on what we decide to value most. I think some Public Forum teams might be wise to consider these underlying values, and arguing that one value truly is of more importance, when confronting terrorism. There is a rich debate to be had here: it's not some foregone conclusion that when the US faces security threats, we should act in favor of security over freedom. In fact, actions taken with this justification, such as the internment of Japanese-American citizens during World War Two, have been incredibly harmful and shameful.

Another option, of course, is to do a costs/benefits analysis approach. Usually this means one side inflates the costs, or benefits, with big number impacts. This approach is a common one nowadays in Public Forum and usually leads to one side or the other, or both sides, actually, being offended at the other team for distorting studies, exaggerating impacts, etc. It's easy to find sources playing the same game of over-claiming everything concerning harms and impacts, on both the left and right, so rounds come down to MSNBC vs. Fox News, not a pleasant thing to watch. Instead, if you choose this route for your framework, I suggest you read analysis from sources like the Atlantic Monthly, Forbes, or the Christian Science Monitor, because their writers are less likely to play this game. The danger is that reasonable, well-supported, warranted claims about harms and benefits are a lot less dramatic and take more explanation, something which may or may not work well with all judges. It's also much harder to quantify the harms/benefits of NSA domestic surveillance, as I have already explained. Still, this probably will be the road most frequently taken, and if you take it, do so reasonably.

The Affirmative

One of the troubling things about this resolution is that it is difficult to find a lot of people praising domestic surveillance by the NSA—other than people who are in charge of the NSA. The NSA leaders, like General Keith Alexander and James Clapper, do present evidence of why the NSA is doing good work, but they do not provide a great deal of analysis to support their claims.

Alexander has essentially argued “we have safeguards to stop any abuse of information gathered” but when pressed for details about those safeguards, says he can’t talk about the classified work his agency does and how it is checked to stop abuses of civil rights. Clapper recently had to apologize for being untruthful in response to congressional testimony but defended himself by saying that he had answered the question about whether or not data from millions of Americans was being collected in the “least untruthful way possible.” Both frequently refer to the Foreign Intelligence Surveillance Act (FISA) courts as the mechanisms by which their agency is checked. But these courts are “secret” courts, and the justifications given by a FISA court are not disclosed publicly. You can find it at [The release of this FISA court decision](#), still heavily redacted, is the exception, not the rule.

For example, Washington Post reporter Andrea Snowden noted, on October 14, 2013:

“Washington Post colleagues Carol Leonnig and Ellen Nakashima, remind us that a key document on the program is still missing from the public disclosures: “the original — and still classified — judicial interpretation that held that the bulk collection of Americans’ data was lawful.” Sources told them that the original document is about 80 pages and was written by Colleen Kollar-Kotelly, then the chief judge of the Foreign Intelligence Surveillance Court.” I read a bit more about Judge Colleen Kollar-Kotelly, and found that she had expressed reservations about how NSA eavesdropping was being used in 2006, according to a Washington Post story (“Secret Court’s Judges Were Warned About NSA Spy Data.” Carol D. Leonnig, Washington Post Staff Writer, February 9, 2006) when she Presiding Judge of FISA courts from 2002-2009... She continues to be a judge for the United States District Court for the District of Columbia, and has published several important decisions, all of which are public and can be read, discussed, and debated. This is not true, however, of her FISA court decision.

It’s hard to provide support of why domestic surveillance is justified when the justifications are kept secret. Benjamin Wittes, a Brookings Institute writer, does give a strong argument, however, to justify mass low-level surveillance: “The NSA can collect a gargantuan quantity of telephone and internet data without violating any statutory or constitutional law. And nearly all of the current debate involves activity that either clearly or arguably falls on the legal side of the line. To the extent that people argue against the legality of what the NSA is doing, they are generally arguing that the courts should have ruled other than the way they did. But in our society, what defines an agency’s legal authority is what the courts actually ruled, not what later critics think they should

have ruled.” (Benjamin Wittes, Lawfare, “Five In Your Face Thoughts in Defense of the NSA.” September 9, 2013)

Wittes believes that pretty much every claim that civil liberties have been violated is based on oversimplification and misunderstanding about what the NSA does, and states that the outcry over Snowden’s revelations is overblown, since abuse of surveillance is self-reported by the NSA and then corrected. In another Lawfare article, he states, “I have gone through the declassified documents very carefully, and these disclosures to my mind show no evidence of any intentional spying on Americans or abuse of civil liberties. They show a remarkably low rate of the sort of errors that any complex system of technical collection will inevitably produce. They show robust compliance procedures. They show earnest and serious efforts to keep the Congress informed, notwithstanding some members’ protestations that they were shocked to learn that NSA—having repeatedly informed Congress that it was engaged in bulk metadata collection—was actually telling the truth. And they show a remarkable dialog with the FISC about the parameters of the agency’s legal authority and a real commitment both to keeping the court informed of activity and to complying with the FISC’s judgment. The FISC, meanwhile, in these documents looks nothing like the rubber stamp that it’s portrayed to be in countless caricatures. It looks, rather, like a serious judicial institution of considerable energy.”

Still, these justifications—our courts have ruled this kind of data collection legal—don’t necessarily prove that the courts should have ruled such data collection legal, as he admits, but dismisses (take a look at the first quotation from him once again). This is one of the reasons I think an old school Lincoln-Douglas values debate approach could be useful on this resolution, because that question would be exactly what one would attempt to answer yes or no on the two sides of the resolution. Finally, Wittes avoids the fact that such massive collection of data, for no reason other than the fact that the data is there to be collected, has never been justified publically by a US court. Remember, the court decision by Judge Colleen Kottar-Kottelly which justified this kind of data collection, under FISA, remains classified. There are some of the problems inherent to arguing affirmatively, especially without a lot of concrete evidence that NSA domestic surveillance has yielded results that were beneficial in the prevention of actual terrorist plots. I haven’t had very long to search for better evidence of such benefits, and I would advise Public Forum debaters to keep looking for that evidence.

Lots of people will probably argue about how we already give up our privacy willingly all the time, via social media, etc. and therefore it’s no big deal that government does the kind of data collection it does. I probably shouldn’t dismiss this argument as much as I do, but the fact is that Google and Facebook can use our information to give it to marketers who try to sell us things. That’s annoying, but not at all the same as the government using our phone records, Google searches, Facebook posts, and emails to see if we might be suspect for targeting in a criminal investigation.

I'm not going to be anything but blunt: affirming this resolution will most likely be much more challenging than negating.

The Negative

One thing the negative could do is argue that the benefits don't outweigh harms simply because there have been few, if any, benefits of NSA domestic surveillance. An Oct. 8, 2013 article by Yochai Benkler for the Guardian.com reports on an exchange during recent Congressional testimony between Senator Leahy (D-Vermont) and NSA chief Alexander:

"Leahy then demanded that Alexander confirm what his deputy, Christopher Inglis, had said in the prior week's testimony: that there is only one example where collection of bulk data is what stopped a terrorist activity. Alexander responded that Inglis might have said two, not one.

In fact, what Inglis had said the week before was that there was one case "that comes close to a but-for example and that's the case of [Basaaly Moalin](#)". So, who is Moalin, on whose fate the NSA places the entire burden of justifying its metadata collection program? Did his capture foil a second 9/11?

A cabby from San Diego, Moalin had emigrated as a teenager from Somalia. In February, he was convicted of providing material assistance to a terrorist organization: he had transferred \$8,500 to al-Shabaab in Somalia.

After the Westgate Mall attack in Nairobi, few would argue that al-Shabaab is not a terrorist organization. But al-Shabaab is involved in a local war, and is not invested in attacking the US homeland. The indictment against Moalin explicitly stated that al-Shabaab's enemies were the present Somali government and "its Ethiopian and African Union supporters". Perhaps, it makes sense for prosecutors to pursue Somali Americans for doing essentially what [some Irish Americans did to help the IRA](#); perhaps not. But this single successful prosecution, under a vague criminal statute, which stopped a few thousand dollars from reaching one side in a local conflict in the Horn of Africa, is the sole success story for the NSA bulk domestic surveillance program."

Another argument is that constitutional protections against unwarranted searches should be valued and therefore block mass data collection from American citizens without a warrant based upon reasonable suspicion. Those who argue that information about phone numbers called and received, which is one piece of communication data gathered en masse, is not constitutionally protected, have solid precedent. But the cases which were decided in this manner came as a result of criminal investigations which included "fishing expeditions" such as asking to see phone records or placing devices which recorded such data on the phone lines of people under suspicion for breaking the law, and did not involve seeking phone records from anyone who has a phone. Also, there is something much more intrusive about gathering email messages, text messages, and internet search terms used, because the data there is much more than numbers and duration times of calls. The fact that the government can gather this sort of data is clear; it is

happening. But it is definitely arguable whether this is consistent with any reasonable interpretation of the 4th amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." There is no particularity to the initial search at all. That much is clear. There is no probable cause to believe that everyone with a phone or email account may be contacting a terrorist organization. The government asserts a right to search, regardless.

This last argument seems to me particularly compelling, but I have to admit that it hasn't held much weight at all in getting changes, for example, in warrantless searches regularly conducted by government officials of the TSA in every US airport.

One other avenue which I believe the negative could take is to challenge the budget cost of implementing the technology and hiring the personnel to analyze the data, but it will be nearly impossible to find exact data about how much it all costs. Such a huge program is bound to be costly, however, and if all it has yielded is arresting one Somalian for sending \$8500 to al-Shabaab, it probably is not worth the investment. Many do argue that traditional law enforcement investigative techniques lead to arrests of terrorists, and that our government policy should be to bolster those efforts instead of sweeping up information about everyone.

Final View

This is definitely a very important topic, but as I have indicated, I believe it will be hard for affirmatives to find great evidence to support current NSA domestic surveillance programs. Perhaps the best idea I have to offer affirmatives is to argue that what the NSA is doing in gathering meta-data is not really surveillance, but something else--a low-level scrutiny of your communication which is making sure, merely, that you aren't calling or emailing terrorists. In other words, the affirmative can try to narrow the topic so that it is about only those within the US who are placed under "targeting" investigation by the NSA after investigators determine that computer programs and analysts have correctly identified a person as deserving of such heightened scrutiny.

That interpretation seems antithetical to the spirit of the resolution, however, so I am not particularly fond of it. The negative, it seems, holds the stronger ground, in opposing current domestic surveillance being conducted by the NSA and confirmed by FISA courts. I hope I am wrong, and that this resolution ends up being equally challenging to affirm or negate.

Topic Analysis by Adam Torson

The tension between civil liberties and national security has once again been brought to the fore by revelations about the scope of NSA domestic spying programs. These programs were made public in information leaked by NSA civilian contractor Edward Snowden, who is now living abroad under threat of arrest by the United States. This is a timely and interesting topic to be sure.

Interpretation and Background

A. NSA Domestic Spying

The National Security Agency is primarily responsible for “signals intelligence,” which means that they intercept and decode electronic transmissions as a means of spying. They are not responsible for “human intelligence” like James Bond or something like that. It is a military institution. The director of the NSA is a military officer and also serves as the head of U.S. Cyber Command, which is the government agency in charge of waging and protecting us from cyber warfare.

The NSA’s domestic spying programs are numerous and extensive, so it’s hard to get a grip on them all. Here are a few we know about so far:

PRISM: NSA collects data from several major technology companies, including Google, Facebook, Microsoft, Yahoo, Apple, YouTube, Skype, and AOL. Information collected includes emails, chat logs, photographs, file transfers, and more.

FAIRVIEW: NSA taps underwater fiber-optic cables to track international internet and phone communications.

BLARNEY: Basically PRISM overseas – the NSA partners with private firms and foreign intelligence agencies to collect the same type of signal intelligence.

XKEYSCORE: This program is a searchable database of signals intelligence collected by the NSA, including metadata and the content of communications. It is stored for a limited period of time but there is a tremendous volume of information – tens of billions of internet records are stored at any given time.

BOUNDLESSINFORMANT: A program designed to assess the amount of information collected by the NSA, it sometimes reports the collection of around 100 billion pieces of intelligence per month.

Controversial revelations have so far included NSA using these programs to map out a person's social connections (there are over 100 requests for Facebook user data per day), NSA officers spying on love interests, NSA bugging the United Nations (in violation of the law), and violations of privacy rules and court orders thousands of times per year.

B. Legal Background

1. FISA (Foreign Intelligence Surveillance) Court

The FISA court was created to issue warrants for foreign intelligence purposes. It is supposed to ensure that the appropriate legal requirements have been met to issue such a warrant. It has been the target of a number of criticisms, in particular that it rarely turns down requests. Since it was created in 1979 it has issued approximately 34,000 secret warrants and denied about 11 requests for a warrant. The court meets in secret for obvious reasons, although this also makes critics suspicious of how it is conducted. It has greatly expanded legal doctrines allowing exceptions to normal due process protections in cases related to National Security.

2. Meta-Data

Many defenders of the NSA claim that it only collects meta-data rather than the content of internet communications. This is information such as the IP address of the sender and receiver, the subject line of emails, dates and times communications are sent and received, etc. There is some basis for the belief that it might be legal to collect this type of information *without a warrant*. In *Katz v. United States*, the Supreme Court ruled that the 4th Amendment's protection against unreasonable search and seizure applied to all areas where a person has a reasonable expectation of privacy. This means that information voluntarily revealed to third-parties is *not* protected by the 4th amendment because you cannot reasonably expect it to be private. For example, when you dial a telephone number you are giving that information to the telephone company, so law enforcement can learn what phone numbers you have dialed without a warrant.

Applying similar logic to electronic communications, just about every single communication on the internet is shared with a third-party. When you send an email you give information to at least your service provider and the recipient's service provider to deliver it to the right place. Others criticize

this logic, saying that in the modern world you can't communicate at all without providing it to a third-party, making the 4th amendment practically meaningless.

Affirmative Positions

A. Terrorism

Far and away the most common advantage to affirming will be preventing terrorism. There are a number of angles the affirmative may take on this issue.

First and most directly, increased surveillance makes it more likely that intelligence agencies will discover communications between individuals plotting a terrorist attack and be able to stop that attack before it happens. Whether this happens very much is a little hard to verify because of course these agencies don't make it public when they use a surveillance program to foil a terrorist plot. There has been some controversy about whether the number of plots foiled indicated in NSA Director Michael Hayden's testimony before congress is accurate. In any case it seems reasonable to suggest that as a general rule more law enforcement and military vigilance makes stopping a terrorist act more likely.

Second, NSA surveillance may make terrorist acts more costly and therefore less likely. When terrorists know that any communication through conventional channels might be monitored, they are forced to recruit and deploy telecommunications and computer experts to circumvent the surveillance mechanisms. Because these high value skills are relatively rare, and cooperating with terrorist groups provides little reward relative to a lawful career in the tech industry, evading conventional means of communication can be a significant barrier to terrorist activity.

Alternatively, terrorist organizations may be forced to rely on low-tech solutions to coordinate their efforts, spread their message, and execute attacks. Lesser sophistication, in turn, makes attacks less frequent and less deadly, and certainly limits the once global scope of these organizations. When you have to use personal messengers instead of cell phones and email, it is very difficult to coordinate an attack involving multiple individuals, training, international money transfers, etc.

Third, NSA domestic surveillance makes it more likely that "home grown" terrorists will be detected and stopped before they can attack. The term "home grown terrorist" refers to a citizen of the United States who is sympathetic to or indoctrinated by the ideologies of terrorist groups. These individuals use their unique access to U.S. targets and their ability to move undetected as a way to facilitate an attack. Depending on your perspective the Boston marathon bombing may

fall into this category. For obvious reasons the fear of home grown terrorism is significant because it is so hard to interdict. Attackers have legal U.S. documents, legitimate reasons to access sensitive sites, and don't fit the stereotype that comes to mind for most Americans when they picture terrorists.

Fourth, NSA programs use digital surveillance to track communications networks and webs of personal associations. This makes detection efforts more sophisticated because the government can track not only communications about the use of violence, but also take a closer look at that individual's known associates. In other words, NSA surveillance strengthens our ability to track terrorist *networks* in addition to just individual terrorists. This is a very powerful tool because virtually nobody carries out a terrorist attack without extensive support and coordination from others. Happening onto one suspicious communication or individual can reveal a treasure trove of valuable intelligence information.

B. Social Contract

The theory of the social contract suggests that people give up certain individual rights in exchange for government's agreement to protect them. Depending on your fundamental beliefs about human nature, this idea might yield a variety of governments. If people are less trustworthy and more conflictual by nature, it might make sense to have a stronger government with fewer protections for individual liberty, as those liberties are likely to be abused to harm others. This most closely resembles the social contract philosophy of Thomas Hobbes and contemporary authors who share his views. Under these circumstances in the modern world a significant security apparatus is probably justified. As people become more capable of harming one another through the use of modern technology, the government's ability to suppress the resulting violence has to grow proportionately. So, if safety in the modern world requires the types of programs deployed by the NSA, then they may be justified.

C. Reasonable Search and Seizure

One of the core negative arguments on the topic will be that NSA domestic surveillance violates the 4th Amendment prohibition on unreasonable search and seizure. There are a few arguments that the affirmative can deploy to answer these objections.

First, the affirmative might deploy the analysis described above about whether electronic communications are even covered by the fourth amendment at all. At least in relation to metadata, advocates of the program argue that what the NSA collects is no different than the

address on the outside of an envelope. The information is turned over to a third party for the purpose of delivering it, and so there is no claim to privacy in that information.

Second, many fourth amendment doctrines allow relaxed warrant requirements for special circumstances where getting a warrant is impractical. For example, most searches that take place when individuals cross the border into or out of the United States do not require the government to secure a warrant. Similarly, many searches in schools or when traveling through airport security do not require a warrant. Perhaps there is an argument to be made that monitoring the metadata of overseas communications is a special circumstance and does not sink to the level of “unreasonable.”

Negative Arguments

There is a tangle of related rights which make the case for the primacy of liberty over safety in questions of national security. I will treat them separately, but you will see a lot of overlap in the analysis. This should suggest to you that each section could be a component of a successful case position.

A. Privacy

1. Privacy as a Political Right

The most obvious right implicated by the topic is the right to privacy. Privacy is important for our own sense of security and individuality. If people feel they are constantly observed they are likely to avoid doing things that others will regard as weird or unusual, including things that are in fact extraordinary and interesting. Their thinking stultifies for fear of harassment or ostracism. Constant observation also affects our sense of safety. When we are constantly observed and treated as a suspect, it is difficult to simply relax and feel at home.

This dynamic is particularly true in the realm of internet communications. The internet has revolutionized the way we learn by allowing people to pursue their own educational interests at any time of the day or night. If people know their search queries and web history are tracked, they will become concerned with how someone might *misinterpret* what they are doing and so avoid learning at all. If our most intimate communications to family and friends can be tracked, we lose the most important part of those relationships, which is the ability to be open and honest and vulnerable. If a researcher visits web forums for white supremacy groups or radical Islamists, are her communications subject to extra scrutiny? Are her friends? If a recent immigrant makes

frequent calls to family in Saudi Arabia or Pakistan, are these grounds for issuing a secret warrant? Do members of an email group devoted to the study of Marxism get an extra pat-down at the airport? Can a high school debater share arguments about Guantanamo Bay without attracting the attention of the Pentagon? These concerns drive privacy advocates in opposing NSA programs.

2. Privacy as a Legal Right

The Constitution does not contain an explicit protection for privacy as such, but it does contain several guarantees of privacy in particular circumstances. For example, the 4th amendment guarantees that a person should be secure in her “person, houses, papers, and effects,” from unreasonable search and seizure, and that a warrant should usually be required to invade this privacy. The 5th Amendment includes the protection against self-incrimination, which protects a person’s right to private thoughts and prevents coerced confessions. The 1st amendment has been interpreted to include a right to freedom of association, which suggests the right to join and advance the interests of private groups without harassment or government regulation. On the view that these and other rights demonstrate that privacy is a constitutional value, the Supreme Court has held that the right to privacy also extends to cases not explicitly mentioned in the Constitution. For example, in *Griswold v. Connecticut*, the court held that states could not outlaw the sale of contraceptives to married people on the grounds that this interfered too significantly with their personal, private lives. The same basic argument was used to justify constitutional protection for the possession of pornography within certain limits (*Stanley v. Georgia*), the right to an abortion (*Roe v. Wade*), the right to live with close family (*Moore v. City of East Cleveland*), and the right to refuse life-saving or life-prolonging medical treatment (*Cruzan v. Missouri Department of Health*).

The idea of a Constitutional right to privacy is a controversial one given that the protections deriving from it are not explicit in the document. Nevertheless, Negatives will be able to rely on a long line of cases finding that such a right is an important protection implicit in the Bill of Rights.

B. Freedom of Association

As indicated above, another political value implicit in the Constitution is the idea of freedom of association. On this view, freedom means more than simply the absence of government restraint or coercion. Freedom is most meaningful when we can join together with others to pursue our common purposes and values. NSA domestic surveillance undermines freedom of association in much the same way that it undermines privacy. By tracking online connections, these programs

make individuals afraid to associate with individuals considered marginal, weird, different, or controversial. They worry about what kind of faulty inferences can be drawn from their associations, and what innocent associations might be used to embarrass or blackmail them. The result is a society that is in fact much less free to associate than it appears on the surface.

C. Freedom of Speech

When people fear that they will be ostracized or harassed for expressing their ideas, they are less likely to do so. Government surveillance creates precisely this risk. Free speech is not only a means to convey your beliefs to others; it is also a tool to explore new ideas, advance controversial beliefs provisionally, provoke reactions from others, and otherwise participate in democratic politics. Constant monitoring of expression creates the prospect of censorship, or worse yet self-censorship.

D. Military Law Enforcement

Another Constitutional concern is the fact that the NSA is a military institution. Domestic law enforcement is the task of the Justice Department through agencies like the FBI, U.S. Marshalls, and ATF. These are organizations with long history and training in methods of criminal detection and interdiction that are consistent with due process norms. When the military is surveilling domestic communications for counter-terrorism operations, is it fighting a war (for which no due process norms apply), or becoming a domestic law enforcement agency? There are significant questions as to whether this type of activity is legal under federal law or under the Constitution. Critics charge that militarizing law enforcement is akin to martial law, which justifies a significant expansion of executive power and much less transparency in federal law enforcement.

E. Intelligence Overload and Overreliance

There are also some more practical concerns about NSA surveillance. Some worry that focusing too much on data collection and analysis makes it impossible to meaningfully process all the data. Information is collected in such massive quantities and destroyed so quickly that many worry that it will at best fail to improve our detection capabilities and at worse create data overload, where there is so much information that it is hard to separate genuine threats from the background noise of everyday innocent communications.

Additionally, some worry that excessive emphasis on electronic communications will distract intelligence services from more traditional but perhaps more effective means of intelligence

gathering, notably “human intelligence” gathered by operatives on the ground. Critics charge that too much reliance on technology and analytics remove the element of human instinct and judgment that may be integral to properly deploying counter-terrorism assets.

F. Abuse

So far we have talked most about the problems associated with NSA surveillance if it is used properly. Critics’ biggest fears are the ways in which this system could be abused. The basic idea is not new. For instance, officials in the Nixon administration ordered operatives to steal the psychiatric records of Daniel Ellsberg (a man who had released classified documents about the Vietnam War) with the hope of finding information that could be used to discredit him. Imagine powerful leaders with similarly nefarious motives having access to a massive system for collecting private information and communications. Military surveillance is, for obvious reasons, a matter of strict secrecy. Checking any kinds of government abuses of this system is virtually impossible. There are already reports from the Snowden leaks which describe an enormous number of illegal acts of surveillance, including NSA staffers tracking information for former love interests. One has to worry that this is just the tip of the iceberg.

Conclusion

This topic is a classic question about the appropriate balance between liberty and national security. Dig in and have fun!

AFFIRMATIVE EVIDENCE

TERRORISM

NSA SURVEILLANCE PREVENTS TERRORISM

Bucci, Steven. [Dr., Director of The Heritage Foundation's Douglas & Sarah Allison Center for Foreign Policy Studies]. "Phone Records and the NSA: Legal and Keeping America Safe," Heritage Foundation. June 20, 2013, <http://blog.heritage.org/2013/06/20/phone-records-and-the-nsa-legal-and-keeping-america-safe/>

U.S. law enforcement and Intelligence agencies depend on tools and methods, such as the leaked NSA program, to combat homegrown radicalization and to fight the ongoing threat from terrorist cells such as the Al-Qaeda in the Arabian Peninsula in Yemen. Moreover, NSA Director General Keith Alexander testified to Congress that these surveillance programs have helped foil dozens of terrorist attacks. These include, he stated, an attempted suicide plot against the New York City subway system by Najibullah Zazi, who pleaded guilty. Since 9/11, the U.S. has thwarted over 50 terrorist plots against America's homeland. In addition to continued reliance on counterterrorism devices such as the Patriot Act and the NSA surveillance programs, Congress must take action to plug the remaining gaps in our counterterrorism system. For instance, there should be increased visa coordination to prevent known terrorists from boarding airplanes and travelling to the U.S. Additionally, Congress should foster greater cooperation among local, state, and federal agencies to streamline their information-sharing capabilities. The current debate raging over Snowden's leaking of the secret NSA surveillance program is no doubt a healthy exercise for a thriving democracy. The scope of the metadata collection and how the government uses it should come under close scrutiny. However, Congress and the American people should understand that these programs—which are under judicial, executive, and legislative oversight—are vital tools for law enforcement and intelligence officials in countering the ongoing threat of terrorism.

NSA SURVEILLANCE HAS PREVENTED 50 ACTS OF TERRORISM

Bucci, Steven. [Dr., Director of The Heritage Foundation's Douglas & Sarah Allison Center for Foreign Policy Studies]. "NSA Spying Stops Terrorism but Should Also Respect Liberties," Heritage. June 18, 2013, <http://blog.heritage.org/2013/06/18/nsa-spying-stops-terrorism-but-should-also-respect-liberties/>

General Keith Alexander, the director of the National Security Agency (NSA), testified in an open hearing before the House Permanent Select Committee for Intelligence on how intelligence collection supports the national effort to fight transnational terrorism. For the first time, he revealed that more than 50 incidents of potential terrorism were stopped by the set of programs under scrutiny. He emphasized that he was working to declassify these incidents so they could be shared with the American people. These revelations come as no surprise to us. Heritage research has noted 54 foiled terrorist plots since 9/11. Given that we know of only three that were not stopped by intelligence (the shoe bomber, the underwear bomber, and the Times Square bomber), this means that these NSA programs might well have played a significant role in thwarting dozens of uncovered plots. Heritage has long held that tools such as the PATRIOT Act and legitimate surveillance programs can be important tools for battling transnational terrorism.

DIGITABLE SURVEILLANCE IS NECESSARY FOR EFFECTIVE COUNTERROR EFFORTS

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>

Cyberspace is the natural battleground for enhanced analytical tools that are enabled by the technology of data collection. If our goal is to combat terrorists or insurgents (or even other nations) then the cyber domain offers us the capacity not just to steal secret information through espionage, but to take observable public behavior and information and use cyber tools to develop a more nuanced and robust understanding of their tactics and intentions. Likewise, it can be used by our opponents to uncover our own secrets. Traditionally, the concept of "surveillance" has been taken to mean an act of physical surveillance—e.g., following someone around or planting a secret camera in an apartment. As technology improved, our spy agencies and law enforcement institutions increasingly came to rely on even more sophisticated technical means of surveillance,[5] and so we came to develop the capacity to electronically intercept telecommunications and examine email while in transit.[6] To these more "traditional" forms of surveillance we must now add another: the collection and analysis of personal data and information about an individual or organization. Call the phenomenon "dataveillance" if you wish, but it is an inevitable product of our increasing reliance on the Internet and global communications systems. One leaves an electronic trail almost everywhere you go. Increasingly, in a networked world technological changes have made personal information pervasively available. As the available storehouse of data has grown, so have governmental and commercial efforts to use this personal data for their own purposes. Commercial enterprises target ads and solicit new customers. Governments use the data to, for example, identify and target previously unknown terror suspects—to find so-called clean skins who are not in any intelligence database. This capability for enhanced data analysis has already proven its utility and holds great promise for the future of commercial activity and counter-terrorism efforts.

THE DATA IS VERY HELPFUL TO INVESTIGATIONS

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>

Compare that condemnation with the universal criticism of the government for its failure to "connect the dots" during the Christmas 2009 bomb plot attempted by Umar Farouk Abdulmutallab.[8] This gives you some idea of the crosscurrents at play. The conundrum arises because the analytical techniques are fundamentally similar to those used by traditional law enforcement agencies, but they operate on so much vaster a set of data, and that data is so much more readily capable of analysis and manipulation, that the differences in degree tend to become differences in kind. To put the issue in perspective, just consider a partial listing of relevant databases that might be targeted: credit card, telephone calls, criminal records, real estate purchases, travel itineraries, and so on. One thing is certain—these analytical tools are of such great utility that governments will expand their use, as will the private sector. Old rules about collection and use limitations are no longer technologically relevant. If we value privacy at all, these ineffective protections must be replaced with new constructs. The goal then is the identification of a suitable legal and policy regime to regulate and manage the use of mass quantities of personal data.

SURVEILLANCE IS CRITICAL TO PREVENTING TERRORIST ATTACKS

Zuckerman, Jessica [Policy Analyst, Western Hemisphere at Heritage Foundation]. "60 Terrorist Plots Since 9/11: Continued Lessons In Domestic Counterterrorism," The Heritage Foundation. July 31, 2013, <http://www.heritage.org/research/commentary/2013/7/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism>

Maintain essential counterterrorism tools. Support for important investigative tools such as the PATRIOT Act is essential to maintaining the security of the U.S. and combating terrorist threats. Key provisions within the act, such as the roving surveillance authority and business records provision, have proved essential for thwarting terror plots, yet they require frequent reauthorization. In order to ensure that law enforcement and intelligence authorities have the essential counterterrorism tools they need, Congress should seek permanent authorization of the three sunset provisions within the PATRIOT Act.[208] Furthermore, legitimate government surveillance programs are also a vital component of U.S. national security, and should be allowed to continue. Indeed, in testimony before the house, General Keith Alexander, the director of the National Security Agency (NSA), revealed that more than 50 incidents of potential terrorism at home and abroad were stopped by the set of NSA surveillance programs that have recently come under scrutiny. That said, the need for effective counterterrorism operations does not relieve the government of its obligation to follow the law and respect individual privacy and liberty. In the American system, the government must do both equally well.

SURVEILLANCE EMPIRICALLY PREVENTS ATTACKS ON THE HOMELAND

Zuckerman, Jessica [Policy Analyst, Western Hemisphere at Heritage Foundation]. "60 Terrorist Plots Since 9/11: Continued Lessons In Domestic Counterterrorism," The Heritage Foundation. July 31, 2013, <http://www.heritage.org/research/commentary/2013/7/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism>

At 2:50 p.m. on April 15, 2013, two explosions went off at the finish line of the Boston Marathon. The brazen terrorist attack killed three people, injured and maimed hundreds more, and shocked the nation. Despite being long recognized as a potential threat by law enforcement and intelligence, few Americans had considered the use of an improvised explosive device (IED) on American soil. And, due to only a few, and relatively small, attacks since 9/11, the public was not in a state of awareness. Yet, the fact remains that there have been at least 60 Islamist-inspired terrorist plots against the homeland since 9/11, illustrating the continued threat of terrorism against the United States. Fifty-three of these plots were thwarted long before the public was ever in danger, due in large part to the concerted efforts of U.S. law enforcement and intelligence. The Heritage Foundation has tracked the foiled terrorist plots against the United States since 9/11 in an effort to study the evolving nature of the threat and garner lessons learned. The best way to protect the United States from the continued threat of terrorism is to ensure a strong and capable domestic counterterrorism enterprise—and to understand the continuing nature of the terror threat.

SURVEILLANCE IS THE LAST, BEST DEFENSE AGAINST TERRORISM

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "Big Brother isn't watching you," American Enterprise Institute. June 10, 2013, <http://aei.org/article/foreign-and-defense-policy/terrorism/big-brother-isnt-watching-you/>

If the critics don't think the NSA should be collecting this information, perhaps they would like to explain just how they would have us stop new terrorist attacks. Terrorists don't have armies or navies we can track with satellites. There are only three ways we can get information to prevent terrorist attacks: The first is interrogation — getting the terrorists to tell us their plans. But thanks to Barack Obama, we don't do that anymore. The second is penetration, either by infiltrating agents into al-Qaeda or by recruiting operatives from within the enemy's ranks. This is incredibly hard — and it got much harder, thanks to the leak exposing a double agent, recruited in London by British intelligence, who had penetrated al-Qaeda in the Arabian Peninsula and helped us break up a new underwear bomb plot in Yemen — forcing the extraction of the agent. That leaves signals intelligence — monitoring the enemy's phone calls and Internet communications — as our principal source of intelligence to stop terrorist plots. Now the same critics who demanded Obama end CIA interrogations are outraged that he is using signals intelligence to track the terrorists. Well, without interrogations or signals intelligence, how exactly is he supposed to protect the country? Unfortunately, some on the right are joining the cacophony of condemnation from the New York Times and MSNBC. The programs exposed in these leaks did not begin on Barack Obama's watch. When Obama continues a Bush-era counterterrorism policy, it is not an outrage — it is a victory.

SURVEILLANCE IS NEEDED TO PREVENT TERRORISM

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "Yes, publishing NSA secrets is a crime," American Enterprise Institute. June 17, 2013, <http://aei.org/article/foreign-and-defense-policy/defense/intelligence/yes-publishing-nsa-secrets-is-a-crime/>

Many do not realize it, but the law is much stricter with the disclosure of signals intelligence than it is with the disclosure of other classified information. All leaks of classified information are damaging, but the exposure of signals intelligence can be catastrophic. Just think back to World War II. If someone had compromised a human intelligence source, a spy or double agent who had infiltrated the Nazi high command, that asset could lose his life, but we would have lost a relatively small amount of intelligence. But if someone had exposed the allies' top secret ULTRA program — through which we broke the encrypted radio and telegraphic codes used by the Nazi leadership — it could very well have altered the outcome of the war. Signals intelligence is of similar import in the war on terror. We cannot track small terrorist cells with spy satellites. The only way we can disrupt the terrorists' plans is by getting them to tell us their plans. In the absence of interrogation, one of the only ways to do that is through signals intelligence. That is why the NSA's surveillance activities are so essential — and why Greenwald could face prosecution for exposing them.

SURVEILLANCE PROVIDES INFORMATION TO PREVENT A FUTURE 9/11

Yoo, John. [Law Professor at the University of California, Berkeley]. "Why We Endorsed Warrantless Wiretaps," American Enterprise Institute. July 16, 2009, <http://aei.org/article/foreign-and-defense-policy/defense/why-we-endorsed-warrantless-wiretaps/>

It was instantly clear after Sept. 11, 2001, that our security agencies knew little about al Qaeda's inner workings, could not detect its operatives' entry into the country, nor predict where it might strike next. Suppose an al Qaeda cell in New York, Chicago or Los Angeles was planning a second attack using small arms, conventional explosives or even biological, chemical or nuclear weapons. Our intelligence and law enforcement agencies faced a near impossible task locating them. Now suppose the National Security Agency (NSA), which collects signals intelligence, threw up a virtual net to intercept all electronic communications leaving and entering Osama bin Laden's Afghanistan headquarters. What better way of detecting follow-up attacks? And what president--of either political party--wouldn't immediately order the NSA to start, so as to find and stop the attackers? Evidently, none of the inspectors general of the five leading national security agencies would approve. In a report issued last week, they suggested that President George W. Bush might have violated the 1978 Foreign Intelligence Surveillance Act (FISA) by ordering the interception of international communications of terrorists without a judicial warrant. The report also suggests that "other" intelligence measures--still classified only because they are yet to be reported on the front page of the New York Times--similarly lacked approval from other branches of government. It is absurd to think that a law like FISA should restrict live military operations against potential attacks on the United States. Congress enacted FISA during the waning days of the Cold War. As the 9/11 Commission found, FISA's wall between domestic law enforcement and foreign intelligence proved dysfunctional and contributed to our government's failure to prevent the 9/11 attacks.

TERRORISM IS A REAL THREAT - SURVEILLANCE IS REQUIRED TO DEFEAT IT

Yoo, John. [Law Professor at the University of California, Berkeley]. "Privacy or Protection?," The American Enterprise Institute. February 11, 2007, <http://aei.org/article/foreign-and-defense-policy/terrorism/privacy-or-protection/>

Our political leaders should consider new ways of addressing this new type of threat. The NSA's terrorist surveillance program, which seeks to intercept communications into or out of the United States involving a suspected al Qaeda agent, represents an effort to go beyond the terrorism-as-crime approach. Preventing terrorist attacks depends on spotting, in advance, patterns and connections in communications, travel and transfers of funds, rather than for waiting for the attacks to occur. We must allow our intelligence agencies to connect the dots, to gather more data, search more broadly, and pool information among more analysts and agencies. Once it was safe to assume there was little need for any domestic surveillance because we no longer faced any serious communist threat; instead, such activities imperiled the privacy rights of harmless students and protesters. The al Qaeda threat is not imaginary, nor an artifact of history, nor a distant or attenuated concern--it is quite real.

SURVEILLANCE WOULD HAVE PREVENTED 9/11

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "The John Kerry Republicans," Washington Post. July 29, 2013, http://www.washingtonpost.com/opinions/marc-thiessen-house-republicans-nsa-hypocrisy/2013/07/29/a39612f8-f847-11e2-8e84-c56731a202fb_story.html

The fact is, they were right the first time. The NSA asked Congress to approve the telephone metadata program in order to close a specific gap in our intelligence capabilities — one that made the 9/11 attacks possible. In the summer of 2001, the NSA had intercepted calls from two of the 9/11 hijackers — Nawaf al-Hazmi and Khalid al-Mihdhar — to an al-Qaeda safe house in the Middle East whose communications were being monitored. However, because the NSA did not have access to metadata on U.S. telephone calls, intelligence officials had no way to know that the two hijackers were in the United States and that their calls had originated in San Diego. As former NSA director Mike Hayden recently pointed out, "If the metadata program had been in effect in the summer of 2001, al-Hazmi and al-Mihdhar would likely have been rolled up, the plane that hit the Pentagon would not have had these jihadists available for the hijacking, and the entire 9/11 enterprise might have been scrapped by al-Qaeda."

ERR ON THE SIDE OF EXPANSIVE INTELLIGENCE PROGRAMS

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "The John Kerry Republicans," Washington Post. July 29, 2013, http://www.washingtonpost.com/opinions/marc-thiessen-house-republicans-nsa-hypocrisy/2013/07/29/a39612f8-f847-11e2-8e84-c56731a202fb_story.html

After 9/11, the House and Senate intelligence committees conducted a joint inquiry into the intelligence failures that led to the attacks. They concluded that one of the main culprits was the "NSA's cautious approach to any collection of intelligence relating to activity in the United States." Now, after a dozen years without an attack on the homeland, they are being accused of the opposite offense. When terrorist attacks succeed, members of Congress are the first to demand that intelligence officials explain why they failed to "connect the dots." Well, if Congress ends the metadata program, those intelligence officials will have a simple answer: because you took away the field of dots.

TERRORISTS WANT TO ATTACK THE US BUT SURVEILLANCE EFFORTS STOP THEM

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013,
<http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

After 9/11, there was a widespread expectation of many more terrorist attacks on the United States. So far that hasn't happened. We haven't escaped entirely unscathed (see Boston Marathon, bombing of), but on the whole we have been a lot safer than most security experts, including me, expected. In light of the current controversy over the National Security Agency's monitoring of telephone calls and emails, it is worthwhile to ask: Why is that? It is certainly not due to any change of heart among our enemies. Radical Islamists still want to kill American infidels. But the vast majority of the time, they fail. The Heritage Foundation estimated last year that 50 terrorist attacks on the American homeland had been foiled since 2001. Some, admittedly, failed through sheer incompetence on the part of the would-be terrorists. For instance, Faisal Shahzad, a Pakistani American jihadist, planted a car bomb in Times Square in 2010 that started smoking before exploding, thereby alerting two New Yorkers who in turn called police, who were able to defuse it.

ABSENT NSA SURVEILLANCE, THERE WOULD HAVE BEEN MORE ATTEMPTED ATTACKS

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013, <http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

But it would be naive to adduce all of our security success to pure serendipity. Surely more attacks would have succeeded absent the ramped-up counter-terrorism efforts undertaken by the U.S. intelligence community, the military and law enforcement. And a large element of the intelligence community's success lies in its use of special intelligence — that is, communications intercepts. The CIA is notoriously deficient in human intelligence — infiltrating spies into terrorist organizations is hard to do, especially when we have so few spooks who speak Urdu, Arabic, Persian and other relevant languages. But the NSA is the best in the world at intercepting communications. That is the most important technical advantage we have in the battle against fanatical foes who will not hesitate to sacrifice their lives to take ours.

SURVEILLANCE SYSTEMS EXIST BECAUSE THEY WORK

Foust, Joshua. [Fellow at the American Security Project]. "These Programs Exist Because They Work," The New York Times. June 10, 2013,
<http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

While debating the morality and ultimate legality of last week's N.S.A. revelations is important, it is also important to realize why programs like collecting telephone metadata and Prism exist to begin with. In short: people think it works. News stories from 2002 show that the public was demanding the intelligence community "do more" to analyze information and thwart any future terrorist attacks. As a result, many of the barriers between domestic law enforcement and intelligence agencies, built after the 1975 Church Committee hearings, have been removed to make investigations easier. Has removing the "wall" actually helped to prevent terrorist attacks? Anonymous government sources have advanced the claim that Prism – a workflow management tool misreported as a means for collecting information – was instrumental in stopping Najibullah Zazi, who had planned on bombing the New York subway system. Those claims are disputed, at least in part, by public records of the Zazi case.

CIVIL LIBERTIES, PRIVACY, AND CONSTITUTIONAL RIGHTS

NSA SURVEILLANCE IS LEGAL

Bucci, Steven. [Dr., Director of The Heritage Foundation's Douglas & Sarah Allison Center for Foreign Policy Studies]. "Phone Records and the NSA: Legal and Keeping America Safe," Heritage Foundation. June 20, 2013, <http://blog.heritage.org/2013/06/20/phone-records-and-the-nsa-legal-and-keeping-america-safe/>

Over the past week, Snowden has inundated the world with details about the NSA collection of telephone records from companies such as Verizon. However, according to a FISA court order, Verizon was only ordered to hand over "metadata" of the calls it processed. Metadata refers to basic information, including telephone number, location, and duration of the call, and the court order does not authorize the government to access the content of such conversations. There is a growing body of legal precedent for the NSA program. In 1976 the Supreme Court upheld "the third party doctrine," which states that anyone who voluntarily provides information to a third party, such as a telephone service provider, cannot object if it is later turned over to the government. What's more, in 1979, the Supreme Court held in *Smith v. Maryland* that the government did not need a warrant to obtain phone record information as it did for the content of such communications. The information was not constitutionally protected because there was no true expectation of privacy. As a result, metadata collection is not protected under the 4th Amendment and is perfectly legal.

SURVEILLANCE IS LEGAL AND DOESN'T VIOLATE PRIVACY

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The NSA's Phone Collection Order - It May be Legal, but is it Wise?," The Heritage Foundation. June 7, 2013, <http://www.heritage.org/research/commentary/2013/6/the-nsas-phone-collection-order-it-may-be-legal-but-is-it-wise>

First, some details. The order applies only to "meta-data" of calls: the phone numbers called, the location of the cell phone when the call was made, and the time and duration of the call. So the order does not require Verizon to let the NSA monitor the conversations or other content of the calls. Also, the order applies both to international calls and to calls occurring wholly within the United States. Verizon is required to update its compliance "on a daily basis." Finally, though the order disclosed Wednesday applies only to Verizon, the logic of the request supports an inference that similar orders have been issued to other major telecommunications carriers like ATT & Sprint. In short, the order appears to give NSA blanket access to the records of Verizon customers' phone calls –foreign and domestic—made between April 25, when the order was signed, and July 19, when it expires. Of course, if the order is only the latest in a series of orders (as also seems likely), then the access may go back for quite some time. To a large degree this revelation it is not unexpected. We are a country still at war against Al Qaeda and its affiliates. As such, we need to have counterterrorism tools, such as Section 215 of the PATRIOT Act, which was apparently used in this case. And, though we don't yet know the details, it is important to note that since 9/11, the powerful tools have been modified and amended to maximize the protection of civil liberties to the extent possible. Here, the FISA court issued an order allowing for telephone calling data only, not the content of any calls. Such data are critical for link analysis -- connecting the dots between phone numbers in terrorist investigations. That is constitutional.

LOSS OF PRIVACY IS INEVITABLE BUT SURVEILLANCE ENSURES BENEFITS FROM THIS LOSS

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>

Ten years ago, surveying the technology of the time which, by and large, was one hundred times less powerful than today's data processing capacity Scott McNealy, then-CEO of Sun Microsystems, said, "Privacy is dead. Get over it." [14] He was, it seems, slightly wrong. Pure privacy—that is, the privacy of activities in your own home—remains reasonably well-protected. [15] What has been lost, and will become even more so increasingly, is the anonymity of being able to act in public (whether physically or in cyberspace) without anyone having the technological capacity to permanently record and retain data about your activity for later analysis. Today, large data collection and aggregation companies, such as Experian and Axicom, may hire retirees to harvest, by hand, public records from government databases. [16] Paper records are digitized and electronic records are downloaded. These data aggregation companies typically hold birth records, credit and conviction records, real estate transactions and liens, bridal registries, and even kennel club records. One company, Acxiom, estimates that it holds on average approximately 1,500 pieces of data on each adult American. [17] Since most, though not all, of these records are governmental in origin, the government has equivalent access to the data, and what they cannot create themselves they can likely buy or demand from the private sector. The day is now here when anyone with enough data and sufficient computing power can develop a detailed picture of any identifiable individual. That picture might tell your food preferences or your underwear size. It might tell something about your terrorist activity. Or your politics. This analytical capacity can have a powerful influence in law and policy and in particular in revealing links between the cyber personas and the real world activities of individuals. When we speak of the new form of "dataveillance," we are not speaking of the comparatively simple matching algorithms that cross check when a person's name is submitted for review when, for example, they apply for a job. Even that exercise is a challenge for any government, as the failure to list Abdulmutallab in advance of the 2009 Christmas bombing attempt demonstrates. [18] The process contains uncertainties of data accuracy and fidelity, analysis and registration, transmission and propagation, and review, correction, and revision. Yet, even with those complexities, the process uses relatively simple technologically—the implementation is what poses a challenge.

NSA SURVEILLANCE ISN'T ANY WORSE FOR PRIVACY THAN HAVING A FACEBOOK ACCOUNT

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013,
<http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

Granted there is something inherently creepy about Uncle Sam scooping up so much information about us. But Google, Facebook, Amazon, Twitter, Citibank and other companies know at least as much about us, because they use very similar data-mining programs to track our online movements. They gather that information in order to sell us products, and no one seems to be overly alarmed. The NSA is gathering that information to keep us safe from terrorist attackers. Yet somehow its actions have become a "scandal," to use a term now loosely being tossed around. The real scandal here is that the Guardian and Washington Post are compromising our national security by telling our enemies about our intelligence-gathering capabilities. Their news stories reveal, for example, that only nine Internet companies share information with the NSA. This is a virtual invitation to terrorists to use other Internet outlets for searches, email, apps and all the rest. No intelligence effort can ever keep us 100% safe, but to stop or scale back the NSA's special intelligence efforts would amount to unilateral disarmament in a war against terrorism that is far from over.

PRIVACY CONCERNS ARE NOT JUSTIFIED

Posner, Eric. [Law professor at the University of Chicago]. "I Don't See a Problem Here," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

The first objection strikes me as weak. We already give the government an enormous amount of information about our lives, and seem to have gotten used to the idea that an Internal Revenue Service knows our finances, or that an employee of a government hospital knows our medical history, or that social workers (if we are on welfare) know our relationships with family members, or that public school teachers know about our children's abilities and personalities. The information vacuumed up by the N.S.A. was already available to faceless bureaucrats in phone and Internet companies — not government employees, but strangers just the same. Many people write as though we make some great sacrifice by disclosing private information to others, but it is in fact simply the way that we obtain services we want — whether the market services of doctors, insurance companies, Internet service providers, employers, therapists and the rest, or the nonmarket services of the government like welfare and security. Even so, I am exaggerating the nature of the intrusion. The chance that human beings in government will actually read our e-mails or check our phone records is infinitesimal (though I can understand that organizations like the A.C.L.U. that have a legitimate interest in communicating with potential government targets may be more vulnerable than the rest of us). Mostly all we are doing is making our information available to a computer algorithm, which is unlikely to laugh at our infirmities or gossip about our relationships.

THE PROGRAM PREVENTS TERROR ATTACKS THAT PRESENT A BIGGER RISK TO FREEDOM

Nye, Joseph. [Professor of Government at Harvard University]. "Privacy gains the upper hand in the NSA surveillance debate," The Daily Star. August 19, 2013, <http://www.dailystar.com.lb/Opinion/Commentary/2013/Aug-19/227751-privacy-gains-the-upper-hand-in-the-nsa-surveillance-debate.ashx#axzz2hEwSq0Dd>

Rather than demonstrating hypocrisy and acceptance of the erosion of civil liberties, the Snowden disclosures have provoked a debate that suggests the U.S. is living up to its democratic principles in its traditionally untidy ways. America faces a trade-off between security and liberty, but the relationship is more complex than it appears at first glance. The worst threats to liberties come when insecurity is greatest, so modest trade-offs can sometimes prevent greater losses. Even such a great defender of freedom as Abraham Lincoln suspended habeas corpus under the extreme conditions of the American Civil War. And such decisions may not be recognized as mistaken or unjust until later – consider Franklin Roosevelt's internment of Japanese-American citizens early in World War II. In the decade after Sept. 11, 2001, the pendulum of public sentiment swung too far to the security pole; but it has begun to swing back in the absence of major new terrorist attacks. A recent ABC News-Washington Post poll showed that 39 percent of Americans now say that protecting privacy is more important than investigating terrorist threats, up from only 18 percent in 2002. Ironically, the programs that Snowden revealed seem to have helped prevent massive new terrorism events, such as a bomb attack on the New York subways. If so, they may have prevented the implementation of more draconian anti-terrorist measures – thus enabling the current debate.

CIVIL LIBERTIES ARE WELL PROTECTED

Gerecht, Reuel. [senior fellow at the Foundation for Defense of Democracies and a former case officer in the CIA's clandestine service]. "The Costs and Benefits of the NSA," The Weekly Standard. June 24, 2013, http://www.weeklystandard.com/articles/costs-and-benefits-nsa_735246.html

But journalists in Washington, who rub shoulders every day with national-security types, surely know that America isn't that far gone. Civil liberties after 12 years of the global war on terrorism are actually as strongly protected in America as they were in 1999, when Bill Clinton was treating terrorism as crime and his minions were debating the morality of assassinating Osama bin Laden. The same is true in France and Great Britain, liberal democracies that have the finest, but also the most intrusive, counterterrorism forces in the West. Surveillance in these countries is intimate—the French internal-security service, the DST, and British domestic intelligence, MI5, bug and monitor their countrymen in ways that remain unthinkable in the United States. Yet the political elites and the societies of both countries have become much more sensitive to, and protective of, personal freedom as their internal security forces have grown more aggressive. It's an odd and, for those attached to Friedrich Hayek's Road to Serfdom, disconcerting development: The massive American government, born of the welfare state and war, hasn't yet gone down the slippery fascist slope. Liberal welfare imperatives may be bankrupting the country, but they have not produced a decline of most (noneconomic) civil liberties. Just the opposite. American liberalism's focus on individual privacy and choice has, so far, effectively checked the creed's collectivism. America's national-security state, which Greenwald believes has already become a leviathan, is, for the most part, rather pathetic.

GOVERNMENT SECRECY

SECRET GOVERNMENT PROGRAMS ARE NECESSARY AND EFFECTIVE

Posner, Eric. [Law professor at the University of Chicago]. "The Secrecy Paradox," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

The question raises a real paradox. If government can keep secrets, then the public cannot hold it to account for its actions. But if government cannot keep secrets, then many programs — including highly desirable ones — are impossible. Many commentators seem to think that the answer is to keep secrecy to an absolute minimum, but this response is far too easy. One reason it is too easy is that it implies that secrecy can be exceptional. Government secrecy in fact is ubiquitous in a range of uncontroversial settings. To do its job and protect the public, the government must promise secrecy to a vast range of people — taxpayers, inventors, whistle-blowers, informers, hospital patients, foreign diplomats, entrepreneurs, contractors, data suppliers and many others. But that means that the basis of government action, which relies on information from these people, must be kept secret from the public. Economic policy is thought to be open, but we saw during the financial crisis that government officials needed to deceive the public about the health of the financial system to prevent self-fulfilling runs on banks. Then there are countless programs that are not secret but that are too complicated and numerous for the public to pay attention to — from E.P.A. regulation to quantitative easing. N.S.A. surveillance blends into this incessant, largely invisible background buzz of government activity; there is nothing exceptional about it.

EXPERTS WITH ACCESS TO SECRET INFORMATION PROVE IT WORKS

Foust, Joshua. [Fellow at the American Security Project]. "These Programs Exist Because They Work," The New York Times. June 10, 2013,
<http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

The government, too, faces a Catch-22 in defending itself: discussing the success of these programs would, by design, require removing secrecy about them. If they only work because they're secret, then that's a tough choice to make. At a political level, too, the effectiveness argument is vitally important. Director of National Intelligence James Clapper has called the leaks "literally gut-wrenching," not because he is an evil man who loves violating privacy laws but because he seems to genuinely believe those exposed programs work. The Senate Intelligence Committee chairwoman, Diane Feinstein, too, has claimed that the N.S.A. effectively disrupts terror attacks. Last week's exposure of the N.S.A.'s surveillance programs does not address whether they were effective or not. But they exist because the people who created and oversee it believe they are effective. If we're to end those programs, we should grapple with the possibility that we're also losing the means to prevent future attacks.

A2 ABUSE OF POWER

THE NSA IS AN ACCOUNTABLE PROGRAM

Carroll, Conn. [senior writer for the Washington Examiner]. "Two Steps Back for National Security," The Heritage Foundation. March 12, 2008, <http://blog.heritage.org/2008/03/12/two-steps-back-for-national-security/>

The abject scaremongering by the left on "the NSA's warrantless domestic spying" is not supported by any facts. The details of the program in question have not, and should not, be revealed. But from what we can piece together from the public record, the program in question touched domestic communications only incidentally and there is zero evidence anywhere that anyone innocent Americans have had their telephone calls listened to or their emails read. FISA experts have made it clear the NSA program in question was probably targeted at electronic communications like email. Due to the complexity and interconnectedness of modern communications, it is impossible for telecommunication companies, or the NSA, to instantly determine whether a single packet of information traveling through a wire in the U.S. is purely foreign in nature (someone in Baghdad e-mailing someone in Riyadh) or purely domestic. The NSA uses complex algorithms to determine if a communication is foreign or domestic, but they first require cooperation from a telecommunication company to keep that data.

THERE ARE INTERNAL CHECKS ON PRIVACY LOSS

Rosenzweig, Paul. [Visiting Fellow at Heritage Foundation]. "The State of Privacy and Security - Our Antique Privacy Rules," The Heritage Foundation. August 1, 2012, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>

First, we are changing from a top-down process of command and control rule to one in which the principal means of privacy protection is through institutional oversight. To that end, the Department of Homeland Security was created with a statutorily required Privacy Officer (and another Officer for Civil Rights and Civil Liberties).[46] The more recent Intelligence Reform and Terrorism Prevention Act,[47] and the Implementing Recommendations of the 9/11 Commission Act of 2007[48] go further. For the first time, they created a Civil Liberties Protection Officer within the intelligence community. More generally, intelligence activities are to be overseen by an independent Privacy and Civil Liberties Oversight Board.[49] Indeed, these institutions serve a novel dual function. They are, in effect, internal watchdogs for privacy concerns. In addition, they naturally serve as a focus for external complaints, requiring them to exercise some of the function of ombudsmen. In either capacity, they are a new structural invention on the American scene—at least, with respect to privacy concerns. Second, and perhaps most significantly, the very same dataveillance systems that are used to advance our counter-terrorism interests are equally well suited to assure that government officials comply with the limitations imposed on them in respect of individual privacy. Put another way, the dataveillance systems are uniquely well equipped to watch the watchers, and the first people who should lose their privacy are the officials who might wrongfully invade the privacy of others.

SURVEILLANCE IS LAWFUL AND EFFECTIVE

Thiessen, Marc. [Member of the White House senior staff under President George W. Bush]. "Big Brother isn't watching you," American Enterprise Institute. June 10, 2013, <http://aei.org/article/foreign-and-defense-policy/terrorism/big-brother-isnt-watching-you/>

But instead of being outraged by the damage done by these leaks, critics on the left and right are criticizing the NSA for undertaking activities that are lawful, constitutional and absolutely vital to protecting the country. Calm down, folks. Big Brother is not watching you. During the Bush administration, critics opposed what they called "warrantless wiretapping." Well, the leaked NSA operations are not warrantless. And, in the case of Verizon, they do not even involve wiretapping. The Verizon court order shows that what is being tracked is not the content of the communications but the records of which phone number called which number, as well as the location and duration of the calls. In *Smith v. Maryland*, the Supreme Court held that there's no reasonable expectation of privacy, and thus no Fourth Amendment protection, for the phone numbers people dial (as distinct from the content of the call), because the number dialed is information you voluntarily share with the phone company to complete the call and for billing purposes. Why does the NSA need to collect all that data? One former national security official explained it to me this way: If you want to connect the dots and stop the next attack, you need to have a "field of dots." That is what the NSA is collecting. But it doesn't dip into that field unless it comes up with a new "dot" — for example, a new terrorist phone number found on a cellphone captured in a raid. It will then plug that new "dot" into the "field of dots" to find out which dots are connected to the new number. If you are not communicating with that terrorist, your dot is not touched. But the NSA needs to have the entire field of dots so it can unravel the network connected to that terrorist. In the case of the PRISM program, the NSA is targeting foreign nationals, not U.S. citizens, and not even individuals in the United States. And all of this collection is being done with a warrant, issued by a federal judge, under authorities approved by Congress.

THERE IS NO EVIDENCE OF PROGRAM ABUSE

Boot, Max. [Senior Fellow in National Security Studies at the Council on Foreign Relations]. "Stay calm and let the NSA carry on," The LA Times. June 9, 2013, <http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>

At first blush these intelligence-gathering activities raise the specter of Big Brother snooping on ordinary American citizens who might be cheating on their spouses or bad-mouthing the president. In fact, there are considerable safeguards built into both programs to ensure that doesn't happen. The phone-monitoring program does not allow the NSA to listen in on conversations without a court order. All that it can do is to collect information on the time, date and destination of phone calls. It should go without saying that it would be pretty useful to know if someone in the U.S. is calling a number in Pakistan or Yemen that is used by a terrorist organizer. As for the Internet-monitoring program, reportedly known as PRISM, it is apparently limited to "non-U.S. persons" who are abroad and thereby enjoy no constitutional protections. These are hardly rogue operations. Both programs were initiated by President George W. Bush and continued by President Obama with the full knowledge and support of Congress and continuing oversight from the federal judiciary. That's why the leaders of both the House and Senate intelligence committees, Republicans and Democrats alike, have come to the defense of these activities. It's possible that, like all government programs, these could be abused — see, for example, the IRS making life tough on tea partiers. But there is no evidence of abuse so far and plenty of evidence — in the lack of successful terrorist attacks — that these programs have been effective in disrupting terrorist plots.

ABUSE CONCERNS ARE ENTIRELY BASELESS

Posner, Eric. [Law professor at the University of Chicago]. "I Don't See a Problem Here," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

The second objection is a lot more serious. We know that our government is capable of misusing information in this way, as occurred during the Nixon administration. Many people seem to believe that President Obama sent telepathic signals to I.R.S. workers instructing them to harass Tea Party organizations. But I am unaware — and correct me if I am wrong — of a single instance during the last 12 years of war-on-terror-related surveillance in which the government used information obtained for security purposes to target a political opponent, dissenter or critic. That means that, for now, this objection is strictly theoretical, and the mere potential for abuse can't by itself be a good reason to shut down a program. If it were, we would have no government.

DEMOCRACY

SURVEILLANCE DOESN'T UNDERMINE DEMOCRACY - IT HELPS ACTUALLY HELPS IT

Posner, Eric. [Law professor at the University of Chicago]. "The Secrecy Paradox," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

This brings me to another valuable point you made, which is that when people believe that the government exercises surveillance, they become reluctant to exercise democratic freedoms. This is a textbook objection to surveillance, I agree, but it also is another objection that I would place under "theoretical" rather than real. Is there any evidence that over the last 12 years, during the flowering of the so-called surveillance state, Americans have become less politically active? More worried about government suppression of dissent? Less willing to listen to opposing voices? All the evidence points in the opposite direction. Views from the extreme ends of the political spectrum are far more accessible today than they were in the past. It is infinitely easier to get the Al Qaeda perspective today — one just does a Google search — than it was to learn the Soviet perspective 40 years ago, which would have required one to travel to one of the very small number of communist bookstores around the country. It is hard to think of another period so full of robust political debate since the late 1960s — another era of government surveillance.

NEGATIVE EVIDENCE

PRIVACY

NSA SURVEILLANCE UNDERMINES OUR BASIC RIGHT TO PRIVACY

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Privacy Is Worth Protecting," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

Well, Eric, we see this very differently. You think the privacy objection is "weak," but the fact is that many people — I'd venture to say most — feel violated when their personal information is surreptitiously collected by the government. The complaint isn't about "a general sense of creepiness." The complaint is that a fundamental right — a right that society has traditionally protected and that society should protect — has been infringed. Of course we share personal information with government agents all the time. We share financial information with the I.R.S., we share information about our children with public school teachers, and so on. But the fact that we sometimes share discrete categories of information with specific categories of people for narrowly delineated purposes doesn't seem to me to be very relevant. "Privacy" means being able to decide for ourselves whom our information is shared with, and when, and under what conditions. Needless to say, the right of privacy shouldn't trump everything. National security (and other government interests) may justify some narrow intrusions on privacy in some circumstances. The problem with the programs disclosed over last week is that they are so astonishingly broad.

THE PROGRAM IS A MASSIVE INVASION OF PRIVACY

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Our Surveillance Laws Are Too Permissive," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

The Guardian revealed on Wednesday that the government has directed Verizon Business Network Services to hand over an array of sensitive information about every domestic and international phone call made by its customers in the United States over a three-month period. The directive, sanctioned by the secretive court that oversees government surveillance in some national security cases, requires Verizon to tell the government who made each call, whom they called, when they made the call, how long the call lasted, and (maybe) where the parties to the call were located. Reportedly, the N.S.A. has been serving all of the major telecommunications companies with similar "metadata" directives for at least seven years. Whatever else might be said about it, the program surely constitutes one of the most ambitious surveillance efforts ever undertaken by a democratic government against its own citizens. As if that weren't enough, The Guardian and The Washington Post also revealed last week that the N.S.A. has secured direct access to the major Internet companies' central servers. There seems to be some confusion about precisely what the N.S.A. is doing with that access, but The Washington Post reports that the agency is collecting information about surveillance targets believed (with 51 percent certainty) to be outside the United States and about people one and two degrees removed from these targets. So the N.S.A. might focus initially on, say, a British journalist working at Der Spiegel, collecting all of her e-mail communications as well as all uploaded videos, photos, Web surfing data, social media posts — and then collect the same information about all of the contacts in the journalist's address book and then about all of the contacts in their address books.

MISTAKES THAT CAUSE ABUSE AND INVASIONS OF PRIVACY ARE INEVITABLE

Gerecht, Reuel. [senior fellow at the Foundation for Defense of Democracies and a former case officer in the CIA's clandestine service]. "The Costs and Benefits of the NSA," The Weekly Standard. June 24, 2013, http://www.weeklystandard.com/articles/costs-and-benefits-nsa_735246.html

Should Americans fear the possible abuse of the intercept power of the National Security Agency at Fort Meade, Maryland? Absolutely. In the midst of the unfolding scandal at the IRS, we understand that bureaucracies are callous creatures, capable of manipulation. In addition to deliberate misuse, closed intelligence agencies can make mistakes in surveilling legitimate targets, causing mountains of trouble. Consider Muslim names. Because of their commonness and the lack of standardized transliteration, they can befuddle scholars, let alone intelligence analysts, who seldom have fluency in Islamic languages. Although one is hard pressed to think of a case since 9/11 in which mistaken identity, or a willful or unintentional leak of intercept intelligence, immiserated an American citizen, these things can happen. NSA civilian employees, soldiers, FBI agents, CIA case officers, prosecutors, and our elected officials are not always angels. Even though encryption is mathematically easier to accomplish than decryption, the potential for abuse of digital communication is always there—all the more since few Americans resort to encryption of their everyday emails.

ABUSE OF POWER

PROGRAM ABUSE HAS HAPPENED BEFORE AND WILL CONTINUE

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Privacy Is Worth Protecting," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

You say you are unaware of a single instance, since 9/11, in which the government used surveillance to target a political opponent, dissenter or critic. But if the government were using surveillance this way, would officials tell us? So much secrecy surrounds the government's surveillance activities that we simply don't know how often, or in what ways, the government's surveillance powers have been abused. This said, we know enough that we ought to be worried. Here is an article about the Department of Homeland Security conducting inappropriate surveillance of protesters associated with Occupy Wall Street. Here is a report of the Justice Department's inspector general finding that the F.B.I. monitored a political group because of its anti-war views. Here is a story in which a former C.I.A. official says that the agency gathered information about a prominent war critic "in order to discredit him."

PROGRAM ABUSE IS INEVITABLE

Goldberg, Jonah. [contributing editor to National Review, named by the Atlantic magazine as one of the top 50 political commentators in America]. "Civil libertarians' hypocrisy," American Enterprise Institute. July 8, 2013, <http://aei.org/article/politics-and-public-opinion/civil-libertarians-hypocrisy/>

"At least 850,000 people have security clearances that give them access to this information," Tiffiniy Cheng of Fight for the Future recently wrote on The Huffington Post. "That's the size of Boston. Imagine if they leak information about a politician or business leaders' personal life — what about a prominent activist? The opportunities for abuse and blackmail are endless; despite what some members of Congress have claimed, the history of government surveillance programs is riddled with abuses." Farhad Manjoo of online Slate magazine agrees. The "fundamental problem" with the NSA's surveillance program is that it's amassing an all-too-tempting stockpile of information. "Someone has access to that data, and that someone might not be as noble as (Edward) Snowden. He could post everything online. He could sell it to identity thieves. He could blackmail you. Or he might blackmail politicians, businesspeople, judges, TSA agents, or use the data in some other nefarious way." One needn't be a privacy absolutist, never mind a paranoid conspiracy theorist, to believe that this is a legitimate concern. One can even support the NSA's PRISM program and still want significant safeguards against abuse.

SURVEILLANCE INEVITABLY BLEEDS INTO DISCRIMINATION AND PROFILING

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013), http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf

From one perspective, the use of the fruits of data surveillance in this way might look like ordinary marketing. But consider the power that data-driven marketing gives companies in relation to their customers. The power of sorting can bleed imperceptibly into the power of discrimination. A coupon for a frequent shopper might seem innocuous, but consider the power to offer shorter airport security lines (and less onerous procedures) to rich frequent fliers, or to discriminate against customers or citizens on the basis of wealth, geography, gender, race, or ethnicity. The power to treat people differently is a dangerous one, as our many legal rules in the areas of fair credit, civil rights, and constitutional law recognize. Surveillance, especially when fuelled by Big Data, puts pressure on those laws and threatens to upend the basic power balance on which our consumer protection and constitutional laws operate. As Professor Danielle Citron argues, algorithmic decisionmaking based on data raises issues of "technological due process."¹¹⁶ The sorting power of surveillance only raises the stakes of these issues. After all, what sociologists call "sorting" has many other names in the law, with "profiling" and "discrimination" being just two of them.

DEMOCRATIC FREEDOMS

SURVEILLANCE HAS A CHILLING EFFECT ON ALL DEMOCRATIC FREEDOMS

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Privacy Is Worth Protecting," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

These abuses are real, but if we focus on them exclusively we risk overlooking the deeper implications of pervasive government surveillance. When people think the government is watching them, or that it might be, they become reluctant to exercise democratic freedoms. They may be discouraged from visiting officially disfavored Web sites, joining controversial political groups, attending political rallies or criticizing government policy. This is a cost to the people who don't exercise their rights, but it's a cost to our society, too. The chilling effect of surveillance makes our public debates narrower and more inhibited and our democracy less vital. This is the greater threat presented by the kinds of programs that were exposed this past week.

SURVEILLANCE CREATES A CULTURE OF FEAR AND DISTRUST

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Democracy Requires Public Accountability," The New York Times. June 9, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

Eric, on your last point about the existence or nonexistence of a chilling effect, let me just point you to this recent report about the effect that surveillance by the New York Police Department has had on the Muslim community in and around New York City. The report concludes that "surveillance of Muslims' quotidian activities has created a pervasive climate of fear and suspicion, encroaching upon every aspect of individual and community life." I wasn't surprised by this conclusion. In the 1970s, the Church Committee came to similar conclusions about the effect that government surveillance had had on the political engagement of African-Americans. Your claim about the pervasiveness and banality of government secrecy elides the fact that there are many kinds of secrecy. Not all of them present the same threat to democracy. I don't think our democracy is made weaker by the government's withholding of information about the technical means it uses to effect surveillance. I don't think our democracy is made weaker by the government's withholding of information about the specific targets of its surveillance — so long as the surveillance is in fact limited to specific targets and so long as there is some mechanism that permits the public to evaluate the government's conduct after the investigation is complete. Secrecy about government policy, though, seems to me a very different thing. The whole point of democracy is to make government accountable to the public. How can the public hold government accountable if it doesn't know what the government's policies are? How can the public lobby Congress to amend the Patriot Act if it has no idea how the government has interpreted it? This is why I think that you have it backward when you say that "objections to the secrecy of the N.S.A. program are thus really objections to our political system itself." It's objections to transparency about the N.S.A. program that have this character. The argument that the government shouldn't be required to tell the public what its policies are is an argument that we shouldn't have a democracy.

SURVEILLANCE DESTROYS ACCOUNTABLE DEMOCRACY AND PRIVACY

Auslin, Michael. [resident scholar and the director of Japan Studies at the American Enterprise Institute]. "Big Brother and the end to freedom," American Enterprise Institute. August 23, 2013, <http://aei.org/article/politics-and-public-opinion/big-brother-and-the-end-to-freedom/>

A great piece by David Rieff in Foreign Policy on Thursday discusses "why nobody cares about the surveillance state." The take away Big Question comes in the last two paragraphs: It is important to be clear. Does the public take the revelations of the data-mining scandal as an affront to their liberty? Presumably many, perhaps even most, do. But life is so full of affronts about which one would be an utter fool to imagine that one can do anything. The automated recordings through which one so often has to pay one's bills, arrange an appointment, or try to get information (even whom to speak with to get that information) are an affront. The endless passwords, PINs, and the like are an affront (and are also, by definition, recorded on corporate databases). The ubiquitous CCTV cameras in city centers, a great many of which were installed well before the Sept. 11 attacks as crime-prevention and traffic-control measures, are an affront. And of course, all the petty and not so petty inconveniences and impositions of the post-9/11 world — from the preposterous demand that one show ID when entering not just a government building but almost any office building in America, to the shameless slovenliness and rudeness of Transportation Security Administration employees at every U.S. airport — are flagrant affronts. Even if the long war against the jihadis were to end tomorrow with total victory for the United States, can anyone seriously suggest that any of these measures would be lessened, let alone canceled? The great myth of the past 25 years may be empowerment through technology. But the great truth of the past 25 years has been the rise of the surveillance state, which grows stronger every day — both because of technology itself and because of the control that states and huge corporations have over the technology that people depend upon and love. On one level, everyone knows this, but whether it's because they believe themselves to be immune or because they simply never imagined that the surveillance state had become so all-encompassing, the elites seem to have been particularly surprised and therefore indignant over the scope of the NSA's spying, the ardor with which governments have defended these practices, and their foaming rage at having to defend them in public at all. "This is the way the world ends," T. S. Eliot famously wrote in his great poem *The Hollow Men*, "not with a bang but a whimper." Welcome to the post-democratic world. Oh, and by the way, you've been living in it for quite some time now. Rieff is on to the opiate-of-the-masses question, and it has already been answered in the affirmative. What governments don't yet seem to get (or care about) is the self-inflicted wounds they are making, cultivating huge and growing reservoirs of distrust and cynicism. Society as a whole is being infected and governance will become ever more fraught thanks to the overreach, arrogance, and lack of self-control on the part of elites. As always, liberty will have to find the hidden nooks and crannies through which to flow, slowly wearing down the rocks of state power and control.

NSA SURVEILLANCE IS THE DEATH KNEEL FOR DEMOCRACY

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," 126 Harvard Law Review. 1904 (2013), http://www.harvardlawreview.org/media/pdf/vol126_cohen.pdf

If, as I have argued, the capacity for critical subjectivity shrinks in conditions of diminished privacy, what happens to the capacity for democratic self-government? Conditions of diminished privacy shrink the latter capacity as well, because they impair the practice of citizenship. But a liberal democratic society cannot sustain itself without citizens who possess the capacity for democratic self-government. A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy. Under such conditions, liberal democracy as a form of government is replaced, gradually but surely, by a different form of government that I will call modulated democracy because it relies on a form of surveillance that operates by modulation. Modulation and modulated democracy are emerging as networked surveillance technologies take root within democratic societies characterized by advanced systems of informational capitalism. Citizens within modulated democracies — citizens who are subject to pervasively distributed surveillance and modulation by powerful commercial and political interests — increasingly will lack the ability to form and pursue meaningful agendas for human flourishing.

OPEN, FREE TECHNOLOGY IS NECESSARY TO BE AN ENGAGED CITIZEN

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," 126 Harvard Law Review. 1904 (2013), http://www.harvardlawreview.org/media/pdf/vol126_cohen.pdf

Networked information technologies mediate our experiences of the world in ways directly related to both the practice of citizenship and the capacity for citizenship, and so they configure citizens as directly or even more directly than institutions do. The practice of citizenship requires access to information and to the various communities in which citizens claim membership. In the networked information society, those experiences are mediated by search engines, social networking platforms, and content formats. Search engines filter and rank search results, tailoring both the results and the accompanying advertising to what is known about the searcher and prioritizing results in ways that reflect popularity and advertising payments. Social networking platforms filter and systematize social and professional relationships according to their own logics. Content formats determine the material conditions of access to information — for example, whether a video file can be copied or manipulated, or whether a news forum permits reader comments. Each set of processes structures the practice of citizenship and also subtly molds network users' understanding of the surrounding world.²⁷ To an increasing degree, then, the capacity for democratic self-government is defined in part by what those technologies and other widely used technologies allow, and by exactly how they allow it.

SURVEILLANCE STIFLES INDIVIDUAL INNOVATION AND FREE THOUGHT

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," 126 Harvard Law Review. 1904 (2013), http://www.harvardlawreview.org/media/pdf/vol126_cohen.pdf

Conditions of diminished privacy also impair the capacity to innovate. This is so both because innovation requires the capacity for critical perspective on one's environment and because innovation is not only about independence of mind. Innovation also requires room to tinker, and therefore thrives most fully in an environment that values and preserves spaces for tinkering. A society that permits the unchecked ascendancy of surveillance infrastructures, which dampen and modulate behavioral variability, cannot hope to maintain a vibrant tradition of cultural and technical innovation. Efforts to repackage pervasive surveillance as innovation — under the moniker "Big Data" — are better understood as efforts to enshrine the methods and values of the modulated society at the heart of our system of knowledge production. The techniques of Big Data have important contributions to make to the scientific enterprise and to social welfare, but as engines of truth production about human subjects they deserve a long, hard second look.

SURVEILLANCE CONSTRAINS FREEDOM OF INNOVATION AND EXPERIMENTATION

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," Harvard Law Review. vol. 126, pg. 1904 (2013),
http://www.harvardlawreview.org/media/pdf/vol126_cohen.pdf

When the predicate conditions for innovation are described in this way, the problem with characterizing privacy as anti-innovation becomes clear: it is modulation, not privacy, that poses the greater threat to innovative practice. Regimes of pervasively distributed surveillance and modulation seek to mold individual preferences and behavior in ways that reduce the serendipity and the freedom to tinker on which innovation thrives. The suggestion that innovative activity will persist unchilled under conditions of pervasively distributed surveillance is simply silly; it derives rhetorical force from the cultural construct of the liberal subject, who can separate the act of creation from the fact of surveillance. As we have seen, though, that is an unsustainable fiction. The real, socially constructed subject responds to surveillance quite differently — which is, of course, exactly why government and commercial entities engage in it. Clearing the way for innovation requires clearing the way for innovative practice by real people. Innovative practice in turn requires breathing room for critical selfdetermination and physical spaces within which the everyday practice of tinkering can thrive.

SURVEILLANCE UNDERMINES RIGHTS TO FREE SPEECH AND PRIVACY

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013), http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf

Intellectual-privacy theory explains why we should extend chilling effect protections to intellectual surveillance, especially traditional-style surveillance by the state. If we care about the development of eccentric individuality and freedom of thought as First Amendment values, then we should be especially wary of surveillance of activities through which those aspects of the self are constructed.⁹⁰ Professor Timothy Macklem argues that "[t]he isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and the subversive."⁹¹ A meaningful measure of intellectual privacy should be erected to shield these activities from the normalizing gaze of surveillance. This shield should be justified on the basis of our cultural intuitions and empirical insights about the normalizing effects of surveillance. But it must also be tempered by the chilling-effect doctrine's normative commitment to err on the side of First Amendment values even if proof is imperfect.

SURVEILLANCE INEVITABLY DETERS TRULY FREE SPEECH

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013), http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf

The mechanics of intellectual privacy discussed so far depend upon knowing, or at least fearing, that someone might be watching us. If we have a sense of privacy, even one that turns out to be an illusion, we are less likely to change our behavior under the panoptic gaze. Truly secret and unexpected surveillance, from this perspective, might appear not to violate our intellectual privacy at all. If we have no inkling that we are being watched, if we really do not care that we are being watched, or if we fear no consequences of being watched, it could be argued that our intellectual freedom is unaffected. It can thus be argued that if the NSA Wiretapping Program had never leaked, it would have posed no threat to intellectual privacy. There are two problems with this account. First, no program of widespread surveillance is likely to remain secret forever. At some point, such a program will inevitably come to light, either by being leaked (as happened with the NSA program and the Army surveillance in Laird), or by actions taken pursuant to the program (such as prosecutions or disclosures). The injury suffered by those thus punished would serve as an example to the rest of us, and the mechanisms of intellectual privacy would come into effect at that point.

LEGALITY

NSA SURVEILLANCE IS ILLEGAL

Sanchez, Julian. [research fellow at the Cato Institute]. "NSA Surveillance Violated Constitution, Secret FISA Court Found," The CATO Institute. July 23, 2012, <http://www.cato.org/blog/nsa-surveillance-violated-constitution-secret-fisa-court-found>

Americans are being told that there's no need to worry about the broad surveillance programs authorized by the controversial FISA Amendments Act of 2008. Yet a report from Wired this weekend paints a more disturbing picture: National Security Agency surveillance enabled by the FAA was found "unreasonable under the Fourth Amendment" by the secretive Foreign Intelligence Surveillance Court "on at least one occasion." The court also found that the government's implementation of its authority under the statute had "circumvented the spirit of the law." Despite these troubling rulings from a court notorious for its deference to intelligence agencies, Congress is so unconcerned that lawmakers don't even want to know how many citizens have been caught up in the NSA's vast and growing databases.

NSA SURVEILLANCE VIOLATES THE FOURTH AMENDMENT

Sanchez, Julian. [research fellow at the Cato Institute]. "NSA Surveillance Violated Constitution, Secret FISA Court Found," The CATO Institute. July 23, 2012, <http://www.cato.org/blog/nsa-surveillance-violated-constitution-secret-fisa-court-found>

That first statement is almost certainly a direct reference to Sen. Dianne Feinstein's assertions in a recent report from the Senate Intelligence Committee—which noted that the Court has blessed much of the surveillance under Section 702, the part of the FAA that permits warrantless acquisition of international communications. Given the massive volume of NSA surveillance, however, the fact that some NSA surveillance was held constitutional is much less significant, for purposes of public accountability, than the fact that some of it was unconstitutional. Feinstein's summary of those positive classified opinions was made public weeks ago, apparently without much trouble. Yet only now that the FAA renewal has made it through multiple committees is the public permitted to know—after much tooth-pulling from a senator, via a letter released late on a Friday afternoon—how incomplete that summary really was. It's cause for concern any time government exceeds the bounds of the Fourth Amendment, but it should be truly worrying when it's in the context of mass-scale spying by the NSA. Based on what little we know of the NSA's programs from public reports, a single "authorization" will routinely cover hundreds or thousands of phone numbers and e-mail addresses. That means that even if there's only "one occasion" on which the NSA "circumvented the spirit of the law" or flouted the Fourth Amendment, the rights of thousands of Americans could easily have been violated.

NSA SURVEILLANCE IS AN UNACCEPTABLE INFRINGEMENT OF THE 4TH AMENDMENT

Sanchez, Julian. [research fellow at the Cato Institute]. "NSA Surveillance Violated Constitution, Secret FISA Court Found," The CATO Institute. July 23, 2012, <http://www.cato.org/blog/nsa-surveillance-violated-constitution-secret-fisa-court-found>

Binney argues that when NSA officials have denied they are engaged in broad and indiscriminate "interception" of Americans' communications, they are using that term "in a very narrow way," analogous to the technical definition of "collection" above, not counting an e-mail or call as "intercepted" until it has been reviewed by human eyes. On this theory, the entire burden of satisfying the Fourth Amendment's requirement of "reasonableness" is borne by the "minimization procedures" governing the use of the massive Pinwale database. On this theory, the constitutional "search" does not occur when all these billions of calls and emails are actually intercepted (in the ordinary sense) and recorded by the NSA, but only when the database is queried. This is a huge departure from what has traditionally been understood to be constitutionally permitted. We do not normally allow the government to indiscriminately make copies of everyone's private correspondence, so long as they promise not to read it without a warrant: The copying itself is supposed to require a warrant, except in extraordinary circumstances. It appears almost certain that a very different rule is in effect now, at least for the NSA. It cannot be overemphasized how dangerous such a change would be. Traditionally, a citizen's right to private communication was either respected or violated at the time it occurred: Your rights would be violated in realtime, or not at all, and even in the lawless era of J. Edgar Hoover, only so many citizens could be spied on at once. Under this new regime, the threat to our rights is perpetual. Even if this administration and the next are scrupulous about respecting civil liberties, even if every man and woman currently employed by the NSA is noble and pure of heart, the conversation you have today may well be there for the use or misuse of whoever holds power in ten years, or fifteen, or twenty. Will the incumbent president in 2032 resist the temptation to hunt for dirt in online chats from his opponent's college years—showing greater restraint than so many past presidents? One must hope so—but better to design the rules of a free society so that such leaps of faith aren't required.

SURVEILLANCE VIOLATES CONSTITUTIONAL GUARANTEES OF INTELLECTUAL FREEDOM

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013), http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf

Shadowy regimes of surveillance corrode the constitutional commitment to intellectual freedom that lies at the heart of most theories of political freedom in a democracy. Secret programs of wide-ranging intellectual surveillance that are devoid of public process and that cannot be justified in court are inconsistent with this commitment and illegitimate in a free society. My argument is not that intellectual surveillance should never be possible, but that when the state seeks to learn what people are reading, thinking, and saying privately, such scrutiny is a serious threat to civil liberties. Accordingly, meaningful legal process (that is, at least a warrant supported by probable cause) must be followed before the government can perform the digital equivalent of reading our diaries. But we must also remember that in modern societies, surveillance fails to respect the line between public and private actors. Intellectual privacy should be preserved against private actors as well as against the state. Federal prosecutions based on purely intellectual surveillance are thankfully rare, but the coercive effects of monitoring by our friends and acquaintances are much more common. We are constrained in our actions by peer pressure at least as much as by the state. Moreover, records collected by private parties can be sold to or subpoenaed by the government, which (as noted above) has shown a voracious interest in all kinds of personal information, particularly records related to the operation of the mind and political beliefs.⁹⁵ Put simply, the problem of intellectual privacy transcends the public/private divide, and justifies additional legal protections on intellectual privacy and the right to read freely.⁹⁶ Constitutional law and standing doctrine alone will not solve the threat of surveillance to intellectual freedom and privacy, but they are a good place to start.

A2 TERRORISM

THERE'S NO EVIDENCE THE PROGRAM IS EFFECTIVE

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Needles Are Harder to Find in Bigger Haystacks," The New York Times. June 10, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

Joshua, I agree with you that effectiveness matters. I can't help but be skeptical, though. If these dragnet programs are effective, where's the evidence? As you note, at least one of the success stories identified by anonymous intelligence officials—the story relating to Zazi—seems not to withstand scrutiny. Let's also note that there's no evidence the government has relied on evidence derived from these dragnet programs in criminal prosecutions. If these dragnet programs had been effective, wouldn't we have seen at least a handful of criminal prosecutions? Of course intelligence surveillance has many purposes; gathering evidence of criminal activity is just one of them. Still, shouldn't the apparent absence of any criminal prosecution make us question how necessary the programs really are? Lacking any more solid evidence of success, you fall back on the point that "the people who created and oversee" these programs "believe they are effective." But unfortunately there are many reasons to question the trust you imply we should put in our national security agencies when they tell us, in essence, "we need more power to make you safe."

THE PROGRAM IS INEFFECTIVE AND UNDERMINES DEMOCRACY

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Needles Are Harder to Find in Bigger Haystacks," The New York Times. June 10, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>

It's also worth remembering that the intelligence community's biggest challenge has never been collecting information; the biggest challenge has always been making sense of it. Launching new programs to collect more information can be a good way to pad the pockets of defense contractors and data-miners, but, as many have noted, it isn't usually a good way to identify terrorist threats. The analogy is now a bit threadbare, but it's still useful: You don't find needles by building bigger haystacks. After the NSA launched the warrantless wiretapping program, FBI agents repeatedly complained that they were drowning in useless information. (Eric Lichtblau wrote: "The torrent of tips led [the FBI] to few potential terrorists inside the country they did not know of from other sources and diverted agents from counterterrorism work they viewed as more productive."). One of the 9/11 Commission's most important observations was that the intelligence community had information in the summer of 2001 that could have allowed it to prevent the 9/11 attacks. The problem wasn't that it lacked information, but that it didn't understand the information it had. Finally, "effectiveness" isn't as simple as you make it out to be. A program can be effective in some very narrow sense but also seriously compromise our democracy over the long term. A program can be effective in some very narrow sense but also be fundamentally inconsistent with our values. Again, I agree that the effectiveness question is worth asking. But answering the effectiveness question isn't as simple as asking whether these surveillance programs yielded useful information.

THE PROGRAM ISN'T NECESSARY TO STOP TERRORISM

Bergen, Peter. [CNN's national security analyst and a director at the New America Foundation]. "Did NSA snooping stop 'dozens' of terrorist attacks?," CNN. June 18, 2013, <http://www.cnn.com/2013/06/17/opinion/bergen-nsa-spying/index.html>

Testifying before Congress on Wednesday, Gen. Keith Alexander, director of the National Security Agency, asserted that his agency's massive acquisition of U.S. phone data and the contents of overseas Internet traffic that is provided by American tech companies has helped prevent "dozens of terrorist events." On Thursday, Sens. Ron Wyden and Mark Udall, Democrats who both serve on the Senate Select Committee on Intelligence and have access to the nation's most sensitive secrets, released a statement contradicting this assertion. "Gen. Alexander's testimony yesterday suggested that the NSA's bulk phone records collection program helped thwart 'dozens' of terrorist attacks, but all of the plots that he mentioned appear to have been identified using other collection methods," the two senators said. Indeed, a survey of court documents and media accounts of all the jihadist terrorist plots in the United States since 9/11 by the New America Foundation shows that traditional law enforcement methods have overwhelmingly played the most significant role in foiling terrorist attacks. This suggests that the NSA surveillance programs are wide-ranging fishing expeditions with little to show for them.

THE PROGRAM HAS NOT PREVENTED ANY ATTACKS

Bergen, Peter. [CNN's national security analyst and a director at the New America Foundation]. "Did NSA snooping stop 'dozens' of terrorist attacks?," CNN. June 18, 2013, <http://www.cnn.com/2013/06/17/opinion/bergen-nsa-spying/index.html>

Alexander promised during his congressional testimony that during this coming week more information would be forthcoming about how the NSA surveillance programs have prevented many attacks. A U.S. intelligence document provided to CNN by a congressional source over the weekend asserts that the dragnet of U.S. phone data and Internet information from overseas users "has contributed to the disruption of dozens of potential terrorist plots here in the homeland and in more than 20 countries around the world." The public record, which is quite rich when it comes to jihadist terrorism cases, suggests that the NSA surveillance yielded little of major value to prevent numerous attacks in the United States, but government officials may be able to point to a number of attacks that were averted overseas. That may not do much to dampen down the political firestorm that has gathered around the NSA surveillance programs. After all, these have been justified because they have supposedly helped to keep Americans safe at home.

ATTACKS THAT HAVE BEEN PREVENTED WEREN'T BECAUSE OF THE NSA

Bergen, Peter. [CNN's national security analyst and a director at the New America Foundation]. "Did NSA snooping stop 'dozens' of terrorist attacks?," CNN. June 18, 2013, <http://www.cnn.com/2013/06/17/opinion/bergen-nsa-spying/index.html>

Homegrown jihadist extremists have mounted 42 plots to conduct attacks within the United States since 2001. Of those plots, nine involved an actual terrorist act that was not prevented by any type of government action, such as the failed attempt by Faisal Shahzad to blow up a car bomb in Times Square on May 1, 2010. Of the remaining 33 plots, the public record shows that at least 29 were uncovered by traditional law enforcement methods, such as the use of informants, reliance on community tips about suspicious activity and other standard policing practices. Informants have played a critical role in preventing more than half of the plots by homegrown jihadist extremists since the 9/11 attacks, according to New America Foundation data. For instance, a group of Muslims from the Balkans living in southern New Jersey who were virulently opposed to the Iraq War told a government informant in 2007 they were plotting to kill soldiers stationed at the nearby Fort Dix army base. Other investigations have relied on tips to law enforcement. Saudi student Khalid Aldawsari's plot to attack a variety of targets in Texas in 2011, including President George W. Bush's home in Dallas, was foiled when a company reported his attempt to buy chemicals suitable for making explosives. Standard police work has also stopped plots. Kevin Lamar James, a convert to Islam, formed a group dedicated to holy war while he was jailed in California's Folsom Prison during the late 1990s. James' crew planned to attack a U.S. military recruiting station in Los Angeles on the fourth anniversary of 9/11 as well as a synagogue a month later.

TERRORIST ATTACKS CAN BE PREVENTED OTHER WAYS

Mueller, John. [Professor of International Relations at Ohio State University]. AND Stewart, Mark G. [civil engineer at the University of Newcastle in Australia and a visiting fellow at Cato]. "3 Questions About NSA Surveillance," The Chronicle of Higher Education. June 13, 2013, <https://chronicle.com/blogs/conversation/2013/06/13/3-questions-about-nsa-surveillance/>

A set of case studies of the 53 post-9/11 plots by Islamist terrorists to damage targets in the United States suggests this is typical. Where the plots have been disrupted, as in the Zazi case, the task was accomplished by ordinary policing. The NSA programs scarcely come up at all. When asked on Wednesday if the NSA's data-gathering programs had been "critical" or "crucial" to disrupting terrorist threats, the agency's head testified that in "dozens" of instances the database "helped" or was "contributing"—though he did seem to agree with the word "critical" at one point. He has promised to provide a list of those instances. The key issue for evaluating the programs, given their privacy implications, will be to determine not whether the huge database was helpful but whether it was necessary.

EMPIRICAL EXAMPLES PROVE THE PROGRAM IS NOT BENEFICIAL

Mueller, John. [Professor of International Relations at Ohio State University]. AND Stewart, Mark G. [civil engineer at the University of Newcastle in Australia and a visiting fellow at Cato]. "3 Questions About NSA Surveillance," The Chronicle of Higher Education. June 13, 2013, <https://chronicle.com/blogs/conversation/2013/06/13/3-questions-about-nsa-surveillance/>

There has been a lot of ominous stammering from Congress and the Obama administration about terrorist plots that have been disrupted by the programs. But thus far, only two concrete examples have been mentioned—not a great many for seven years of effort. First, there have been suggestions that the NSA programs helped apprehend an American who had done surveillance work for the terrorist gunmen in Mumbai, India, in 2008. His efforts, however, were of limited importance to the event, and his eventual arrest didn't prevent the attack. The second was the 2009 Zazi case, in which three Afghan-Americans trained in Pakistan before returning to the United States and plotted to set off bombs in the New York subway system. Given the perpetrators' limited capacities, it is questionable whether the plot would ever have succeeded. Furthermore, the plot was disrupted not by NSA data-dredgers but by standard surveillance: British intelligence provided a hot tip about Zazi based on e-mail traffic to a known terrorist address—one that had long been watched. At that point, U.S. authorities had good reason to put the plotters on their radar. Having NSA's megadata collection may have been helpful, but it seems scarcely to have been required. Actually, it is not clear that even the tip was necessary because the plotters foolishly called attention to themselves by using stolen credit cards to purchase large quantities of potential bomb material.

TERRORISTS ARE ADAPTING TO AVOID SURVEILLANCE

Dozier, Kimberly. [staff writer at the Associated Press]. "AL-QAIDA SAID TO BE CHANGING ITS WAYS AFTER LEAKS," The Associated Press. July 26, 2013, <http://bigstory.ap.org/article/al-qaida-said-be-changing-its-ways-after-leaks>

Two U.S. intelligence officials say members of virtually every terrorist group, including core al-Qaida members, are attempting to change how they communicate, based on what they are reading in the media, to hide from U.S. surveillance. It is the first time intelligence officials have described which groups are reacting to the leaks. The officials spoke anonymously because they were not authorized to speak about the intelligence matters publicly. The officials wouldn't go into details on how they know this, whether it's terrorists switching email accounts or cellphone providers or adopting new encryption techniques, but a lawmaker briefed on the matter said al-Qaida's Yemeni offshoot, al-Qaida in the Arabian Peninsula, has been among the first to alter how it reaches out to its operatives. The lawmaker spoke anonymously because he would not, by name, discuss the confidential briefing. Shortly after Edward Snowden leaked documents about the secret NSA surveillance programs, chat rooms and websites used by like-minded extremists and would-be recruits advised users how to avoid NSA detection, from telling them not to use their real phone numbers to recommending specific online software programs to keep spies from tracking their computers' physical locations.

THE PROGRAM IS A HUGE WASTE OF TAX DOLLARS

Mueller, John. [Professor of International Relations at Ohio State University]. AND Stewart, Mark G. [civil engineer at the University of Newcastle in Australia and a visiting fellow at Cato]. "3 Questions About NSA Surveillance," The Chronicle of Higher Education. June 13, 2013, <https://chronicle.com/blogs/conversation/2013/06/13/3-questions-about-nsa-surveillance/>

After 9/11, U.S. intelligence concluded that there were thousands of Al Qaeda operatives in the country. That perspective impelled a vast and hasty increase in spending on intelligence and policing, and at least 263 military and intelligence agencies have been created or reorganized. For its part, the Department of Homeland Security has set up a vast array of "fusion centers" to police terrorism, but is unable to determine how much they cost. It estimates that somewhere between \$289-million and \$1.4-billion were awarded to them from 2003 to 2010—a gap of over a billion dollars that is impressive even by Washington standards. As it turned out, the number of Al Qaeda operatives actually in the United States registered at zero or nearly so, and the threat of terrorism in the country proved to be far more limited than initially feared. Accordingly, there might logically have been some judicious cutbacks in the funds devoted to the expensive quest to find terrorists who mostly didn't exist—a process some in the FBI call "ghost chasing." However, the reaction has continually been to expand the enterprise, searching for the needle by adding more and more hay. Far overdue are extensive openly published studies that rationally evaluate homeland-security expenditures. The NSA's formerly secret surveillance programs have been part of the expansionary process. If they have done little to prevent terrorist attacks in the United States, and if we are now having what President Obama has characterized as a "healthy" debate about the programs, it seems reasonable to suggest that the debaters should at least be supplied with information about how much the programs cost. Knowing the cost would scarcely help the terrorists. It might, however, amaze American taxpayers. Perhaps that's another reason the programs have been kept secret.

SOFT POWER

NSA SURVEILLANCE DEVASTATES OUR INTERNATIONAL CREDIBILITY

Chen, Xiangyang. [Research Fellow, China Institute of Contemporary International Relations]. "Strategic Impacts of the 'Snowden Incident' on International Relations," China US Focus. September 9, 2013, <http://www.chinausfocus.com/peace-security/strategic-impacts-of-the-snowden-incident-on-international-relations/>

Although the fireworks ignited by the "Snowden incident" have dimmed, its strategic impacts on international relations are only beginning to be felt. The incident is affecting the game theory among the world's four leading powers of the US, China, Russia and European Union and leftwing forces in Latin America, involving state and non-state entities operating in cyber-space as well as the real world and reflecting a new characteristic of today's multi-national politics. Due to the incident, three injuries have been inflicted on the US. First, it has seriously hurt the international image of America and somewhat weakened its "soft strength". Secret operations such as "PRISM" have exposed the US double-standard on Internet security and online privacy, and proved beyond reasonable doubt the US hypocrisy over human rights, anti-terrorism and moral leadership. It also demonstrates how easy it is for the US not to match its own words with appropriate action and how porous its intelligence out-sourcing system is. There is no doubt the US will review its entire cyber-snooping system and make whatever improvement necessary. Just two years after WikiLeaks put thousands of classified telecommunications between Washington and US diplomatic missions around the world under the sun, the "Snowden incident" brought more of Washington's dark secrets into public view. Dealing such a heavy blow to the no-holds-barred global electronic surveillance franchise, the damage to US intelligence setup could be comparable to that of "9/11" to national security.

SURVEILLANCE JUSTIFIES AUTHORITARIAN CRACKDOWNS AROUND THE WORLD

Rid, Thomas. [PhD., Reader in War Studies at King's College London]. "The Rest of the Snowden Files Should Be Destroyed," Slate. September 10, 2013, http://www.slate.com/articles/technology/future_tense/2013/09/nsa_surveillance_the_rest_of_the_snowden_files_should_be_destroyed.html

Meanwhile, thirdly, authoritarian states get a confidence boost. "Washington ate the dirt this time," wrote China's Global Times, an outlet sometimes called the Fox News of China. The U.S. administration "has long been trying to play innocent victim of cyberattacks" but now turned out to be "the biggest villain," said Xinhua, the state-run news agency. This argument, of course, is hypocrisy. The National Security Agency is not spying in order to round up Obama's political opposition, and Government Communications Headquarters is not listening to Internet traffic to help London's banks—both of which stand in sharp contrast to China's own practices. Nevertheless, Snowden's revelations make it easier for the world's authoritarian regimes to crush dissent at home. A fourth result: Internet governance is creaking. Diminishing America and Britain's diplomatic and moral standing is threatening the multistakeholder approach, so far a guarantor for a free and open Internet. A patchwork of smaller, sovereign "Internets" is becoming more and more likely. As a result, the Internet could now become more authoritarian, not less.